The Next Four Years: Intelligence Community Reform Refining, not Rebooting

by Frank Strickland and Chris Whitlock

In the next four years the executive and legislative branches will pick up the recurring question of additional intelligence community reform. Did the Intelligence Reform and Terrorism Prevention Act of 2004 get it right? Is a sweeping reorganization of the intelligence community required to "fix the problem"? This article examines these questions and recommends a strategy with specific implementation details. While it is hoped the article will have value inside the intelligence community, it is especially intended for government leaders outside the community whose legislation and policy will drive any additional reform.

Understanding the Problem

The U.S. intelligence community is a collection of 16 agency and departmental organizations executing a roughly $75 billion annual budget. The community's mission to understand the world, warn of crises, and support national security actions—often against cunning and destructive threats—is a difficult one to put it mildly. We can describe the problem of managing intelligence in practical terms by considering it from two aspects: integrating the five functional intelligence disciplines, and applying the intelligence enterprise to the range of national security problems and questions.

The best intelligence requires the integration of five primary types of intelligence—signals (SIGINT), human (HUMINT), open source (OSINT), geospatial (GEOINT), and measurement and signatures (MASINT). This is not simply a matter of integrating the data produced by these five functional disciplines. The "connect the dots" metaphor has little resemblance to the object it seeks to describe. Technologist Jeff Jonas, who is not an intelligence professional, has a metaphor that closely resembles the reality of intelligence problems.

Imagine a giant puzzle with five different types of pieces—the five intelligence disciplines. As you try to fit together these different types of pieces, you eventually realize that pieces of the puzzle are missing. This is the inherent uncertainty in intelligence. There are some facts that determined adversaries will manage to withhold until after the fact or perhaps forever. Worst yet, seemingly legitimate pieces of the puzzle are in fact bogus: they don't belong to the puzzle you are assembling, although you don't immediately recognize this problem as the pieces seem perfectly suited. This is the deliberate deception that cunning adversaries will execute to deceive intelligence about their actual capabilities and intentions. For the hardest targets—weapons of mass destruction, cyber, or terrorists—it takes multiple types of intelligence working together to accurately complete as much of the puzzle as possible, and properly characterize the uncertainty over the missing pieces of the puzzle. Bringing the intelligence disciplines together for this result is the work of intelligence integration.

Intelligence integration does not begin with collected data; it begins with the strategy for solving a problem. What is the customer's problem? How will intelligence address that problem? What are the related intelligence hypotheses and questions? How do we analyze those hypotheses

with indicators and evidence? From an integrated intelligence strategy come collection and analysis focused on the customer's problem, ultimately creating intelligence that is integrated with the customer's operations. One discipline will at times answer part of an intelligence problem, but the best understanding of complex problems requires an integration of multiple intelligence disciplines, much as the brain's understanding of complex environments requires the integration of multiple senses.

Second, consider the breadth and depth of the problems intelligence must address. At the highest level, intelligence problems involve one or more national security topics, such as cyber attacks, presented as problems based on the behaviors of one or more state and non-state actors. Imagine an array of dozens of national security problems against hundreds of state and non-state actors. Of course, every problem-actor intersection does not require intelligence. For example, the problem of weapons of mass destruction (WMD) does not occur in every country, nor does every non-state actor present a WMD threat. However, the high-level priorities at the problem–actor intersection can number well into the thousands. For each of these problems, one can then envision multiple important questions requiring intelligence.

Now, imagine your job is to effectively and efficiently integrate the five functional disciplines against all of the problems in this array. Thus, you have a basic appreciation for the complex depth and breadth of managing intelligence, one of the daily challenges of the director of national intelligence (DNI). This is a problem that must be managed, as it cannot be solved. It is an ongoing challenge that requires more than organizational and budgetary controls.

Reforming by Refining, not Rebooting

Since the National Security Act of 1947, Congress and the executive branch have continuously sought to improve the management of intelligence. In just the past 30 years there have been nearly three dozen studies of how to improve intelligence community management. The Intelligence Reform and Terrorism Prevention Act (IRTPA) is the most recent legislative action to reform the community's performance and management. While the IRTPA has contributed to intelligence improvements, such as increased sharing of data on terrorism, most in and around the intelligence community would assert that managing the intelligence enterprise is still a work in progress.

The DNI has further focused the intelligence disciplines on integrated operations by establishing national intelligence managers (NIMs). These NIMs seek to facilitate integrated intelligence strategies that support national security outcomes. Focusing all of intelligence on security outcomes and the integrated strategies that support those outcomes would seem an unquestionably good thing to do. Yet, the NIM approach is hardly wanting for skeptics and critics.

It may be that no amount of tinkering with organizational and budgetary authorities—or other classic bureaucratic levers—will substantially improve the management of intelligence. If that were the case, surely the issue would be put to rest now after dozens of studies, annual intelligence authorizations dating back to 1978, and the most sweeping piece of national security legislation since 1947 in the 2004 IRTPA.

When considering how to improve the management of intelligence, it is helpful to first recognize that the solution is not an end state. Intelligence, like the threats it confronts, is a living process; one that must constantly change to keep pace with the behavioral changes of the threats, their capabilities and intentions, and the world in which America and our adversaries and allies operate. Thus, improving the management of intelligence is an ongoing process, similar to the continuous improvement efforts required for enterprise management processes in competitive commercial enterprises.

Next, it is equally helpful to keep in mind that enterprise management processes ultimately depend on the personal relationships among the principals. The management of intelligence will never be simply an automated system that spits out answers. It rests first and foremost on the connections between intelligence officers and the customers they serve. The most exquisite requirements system ever imagined cannot offset the importance of these relationships. The relationship between the President and the DNI is the most important of these, but the principle applies down through all customer-intelligence officer relationships. These relationships are closely followed in importance by those between intelligence officers from the functions across the five major disciplines and the hundreds of capabilities within those disciplines. Relationships are developed and nurtured by people, especially leaders, and no amount of statute and policy can substitute for these relationships.

That said, managing an enterprise as large and complex as the intelligence community cannot be done through people and relationships alone, regardless of how competent and interrelated they are. Managing the intelligence enterprise requires many decisions regarding the allocation of operational and fiscal resources for desired security outcomes, assessing the effects of those decisions, and continuously

refining those decisions to achieve the best mix of desired outcomes across the breadth and depth of priorities outlined above. Managing intelligence is by its very nature a data-driven process, and analytics are required to complement the leaders' thinking and interactions.

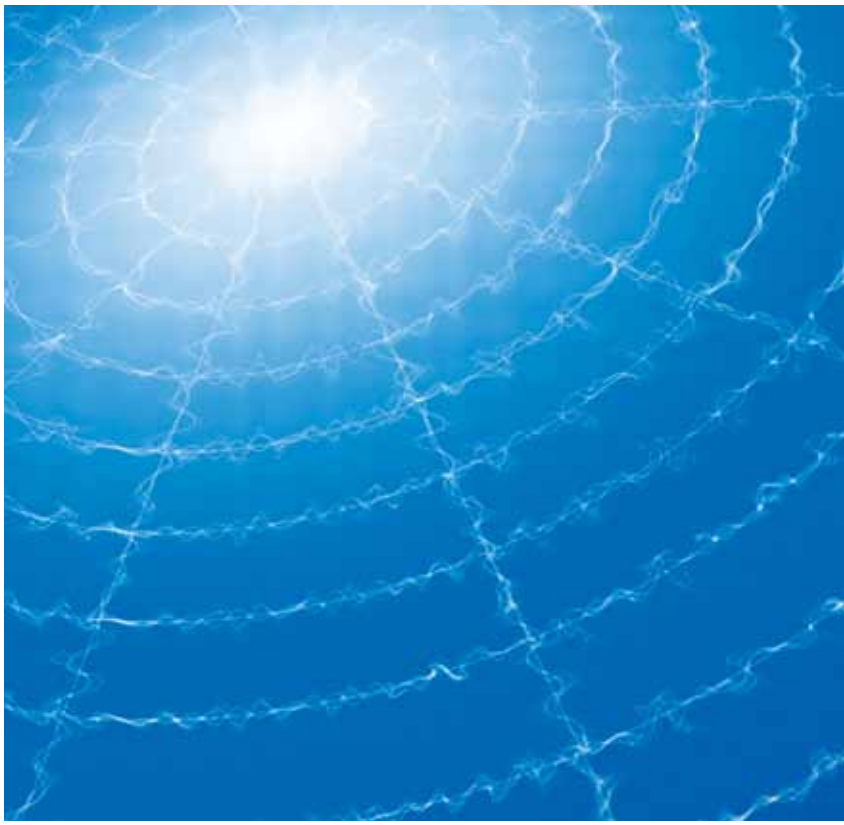
For an enterprise whose primary mission is data-driven analysis of threats, intelligence has been much slower in applying data and analytics to managing the enterprise. Historically, intelligence management was based on the experience and intuition of seasoned intelligence officers and too often on one or a handful of anecdotes. Experiential and intuitive judgment is essential to managing any complex enterprise, but the enterprise management system must serve experience and intuition with hard data and solid analysis.

Looking Forward

Looking into the next decade and beyond, the community faces some tremendous operational challenges. On the one hand, intelligence must become much more open and transparent, especially where speculative questions about the future are concerned. The best information and thinking about this century are not completely within the bounds of the intelligence community. On the other hand, some elements of intelligence must become even more clandestine or covert in order to penetrate the hardest targets. Stealing secrets will always be at the very core of the intelligence mission. Stealing secrets requires secret sources and methods.

The community must address these operational challenges in an era of constrained resources. It is easier to create new capabilities when programs are flush with funding than it will be in the next decade or so, when resources are flat or declining. The intelligence community is a mission-driven culture, one that naturally encourages operational innovation. Innovations in the management of intelligence—especially the allocation of scare operational and fiscal resources across many competing priorities—come less naturally. Perhaps more reforms are necessary to help, but of what type?

One former intelligence agency director characterizes intelligence reform by noting that "the intelligence community has been on the operating table for the past decade." There have been major organization and budget reforms during this time. The community has implemented these reforms while helping protect the American homeland and the nation's interests abroad. Further improvements in the management of intelligence may require different levers.



The IRTPA has driven substantial changes that have improved essential elements of intelligence, such as the sharing of information between agencies. The DNI's focus on the integration of intelligence has further strengthened collaboration among agencies against specific intelligence problems. In terms of an integrated approach to managing intelligence, the NIMs have made strides in promoting strategies, information sharing, and inter-organizational teamwork that better integrate the functional disciplines.

The work of sharing intelligence data and information between agencies will always be a work in progress. Effective intelligence services are continuously conceiving and creating new means to penetrate secrets. This leads to compartmentation which in turn requires ongoing efforts to appropriately share information. This too is a problem to be managed, not solved.

Given the substantial progress made in sharing information—and the tremendous volumes of information available to analysts and managers today—the primary challenge facing both intelligence analysis and the management of intelligence has likely shifted from sharing the data to making sense of it. While one may wish to tweak how enterprise management is organized—such as reducing the number of

NIMs or changing how the NIMs relate to the national intelligence officers—the major improvements in managing intelligence will be found in the use of data and analytics to inform the creation of intelligence strategies and assess how the community is performing against the strategies. Mission performance assessments based on hard data should start to regularly drive the allocation of not only operational capabilities, but budgeting for future capabilities as well.

Achieving this type of reform does not require a major acquisition program or additional staff added to the management processes. Commercial analytics capabilities have matured to the point that they are well suited for making sense of large volumes of disparate data types on the intelligence community's performance. The community and its customers' behaviors are well-instrumented, thanks to the proliferation of modern IT networks and systems. Analytics are able to gather and make sense of data on the community's performance and even how intelligence products are or are not adding value to customers' missions—the ultimate measure. These analytics can move the resource decision-making to a higher plane, away from simply discussing requirements, capabilities, and performance anecdotes to a more comprehensive discussion of intelligence value.

For the cynics, the point here is not that analytics will by themselves determine the value of intelligence or make decisions about resource allocations (although some level of automated resource allocation is entirely possible through automated activity models). The evidence, however, is clear that analytics can greatly improve the quality, timeliness, and coherence of decisions about the value of intelligence and how to get the most from limited intelligence resources against seemingly unlimited national security questions.

Benefits to the Mission

Focusing additional intelligence reforms on this more practical aspect of managing intelligence with analytics has four benefits to the intelligence mission.

Leaders can use data-driven performance assessments to focus the many constituents to any intelligence problem on the customer's need, the performance of intelligence against that need, and the alternatives for improving performance. This will not eliminate conflict in the bureaucracy, but it can help leaders create a culture of constructive conflict and timely decision-making and action, even in a large and complex enterprise.

Analytics can help smaller staffs bring together performance assessments from data available on the networks, minimizing data calls on the operating agencies. Instead of investing time in responding to data calls, operating agencies can engage in the dialogue on the completeness, accuracy, and implications of the performance data. This should have the net effect over time of reducing the size of staff in the enterprise.

Data-driven assessments can help strengthen inter-organizational team performance and further intelligence integration by focusing teams on substantive mission issues clearly defined by data and analysis. This will not eliminate the organizational equities and turf brought to any inter-organizational effort, but it can greatly reduce this impediment to collaboration.

The greatest benefit, perhaps, is that this approach to further reforming the management of intelligence puts an immediate focus on improving the value of intelligence. Major changes in organizations, budgets, and other traditional bureaucratic levers of change are arguably unnecessary, and likely disruptive to the mission for benefits that may or may not come for some time into the future.

Summary

Perhaps the intelligence community requires some additional changes in the traditional elements of government reform. However, given the organizational and budgetary reforms made in the past decade and the mission and fiscal challenges ahead, the next phase of improvements in the management of intelligence will be best served by focusing on the use of data and analytics to assess and improve specific mission problems and the allocation of scarce resources. Performance management analytics will give the intelligence community and its customers the knowledge necessary to allocate operational and fiscal resources in an environment wherein many competing priorities and constrained resources are considered against the consequences of potential failures in our national security capabilities. Further improvements to the management of intelligence require focused refinements, but not a major rebooting of the intelligence community.

TO LEARN MORE

About the Center's Governing in the Next Four Years series, insights from the series are available online at www.businessofgovernment.org/content/governing-next-four-years.