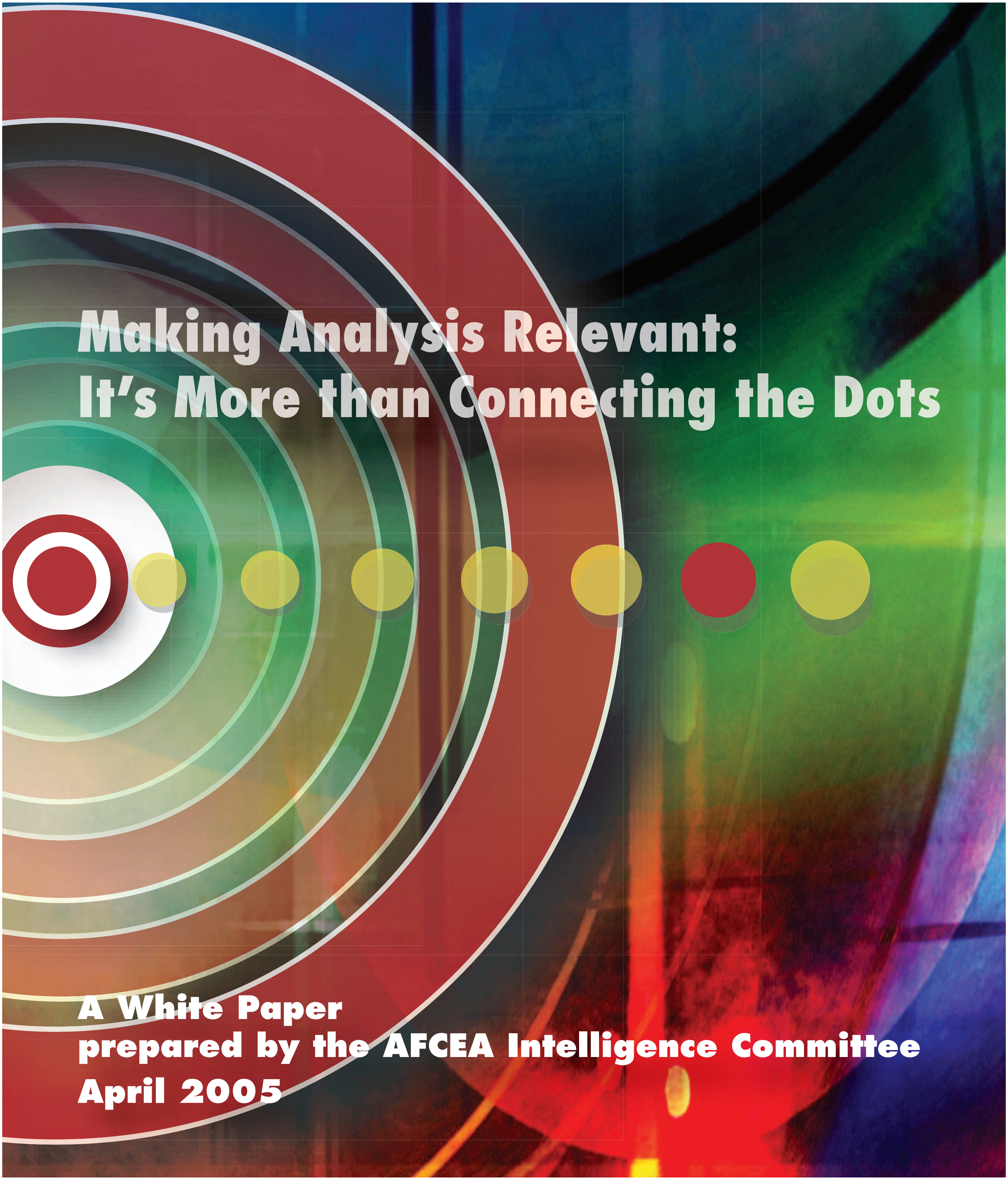

Making Analysis Relevant: It's More than Connecting the Dots

A White Paper
prepared by the AFCEA Intelligence Committee
April 2005

AFCEA *The Association committed to serving the Intelligence Professional*

Making Analysis Relevant: It's More than Connecting the Dots

Introduction

The Intelligence Committee of the Armed Forces Communications and Electronics Association (AFCEA) is pleased to present this third in a series of white papers focused on the future of the Intelligence Community (IC). In authoring these papers, the committee intends to contribute to a national discussion about ways to strengthen the contribution intelligence makes to our nation’s security and to address the growing need for intelligence to function within the evolving operational concepts of defense, homeland security and the other components of national security.

In contrast to our earlier white papers, this offering constitutes a series of shorter topics focused on specific aspects of intelligence analysis. The committee views the Intelligence Reform and Terrorism Prevention Act of 2004 as an opportunity to build a national intelligence capability responsive to the changing international security environment in which our nation must lead. The authors have given serious thought to a variety of approaches to community methodology and organization – and even to organizing principles. Although these papers do not represent a combined recommendation, they do reflect the committee’s view that intelligence analysis can be improved significantly by questioning the traditional intelligence cycle and the organizational structures that support it. The papers commence with a focus on the importance to analysis of understanding the “unknowns” and proceed through discussions that highlight a variety of organizational and analytic issues. The papers close with a call to use the opportunity offered by the establishment of a Director of National Intelligence (DNI) to look at the concepts underlying the intelligence cycle as it is practiced today.

The committee views the current national security environment as both challenging and ripe with promise. We see in the Intelligence Reform and Terrorism Prevention Act a commitment to make the improvements needed in our IC. AFCEA and the committee offer these papers in support of that commitment.

Analyzing the Unknowns

The hulking monster in our analytic living room is the “unknown.” Arguably, it is the leading contributor to intelligence failure; it is the prime source of surprise; and it can lead to policy, strategic or tactical failure. Intelligence is geared primarily to report and analyze what we collect. Our processes that deal with the “unknown” are largely internalized within intelligence operations and drive collection. We do not adequately let the users of intelligence know where we do not have knowledge and what might be the implications of these voids.

The fundamental purpose of analysis is to take bits and pieces of what is known and to use this information to present a more complete picture of what we hope is reality. Often, however, intelligence analysis places too much emphasis on what is collected and inadequately accounts for what is not. We must develop a more sophisticated, consistent, and disciplined approach to reporting and assessing what we do not know. We must create a focused effort to establish processes, procedures and technologies to help.

The business of trying to find out about something (collection) and making sense of it (analysis) is a cycle—a timeless one. Too often, our Community has focused on the mainstream of the analytic portion of this cycle—the analysis of the information we get—and has not placed enough attention on an analysis of the implications of the information we do not have. A way to envision this in terms of the "Intelligence Cycle" is to see an "unknown realm" as an eddy somewhere between collection and analysis—the information never gets into the analytic process because it is not known. It should not be surprising therefore that sometimes our analysts draw too much from the information they have and do not account adequately for the unknowns and the potential impacts of these unknowns on their conclusions and, ultimately, on their customers.

Using the "connect-the-dot" analogy, analysis can be seen as connecting dots (knowns) that are of varying distance and ensuring the lines between the dots are more than simply straight connections, reflecting, as nearly as possible, the actual profile of the line between the two known points (if those points connect at all). When the dots are close enough because of superb collection, the picture of truth is often evident and unambiguous, and the intelligence problem is mostly one of reporting and predicting. The challenge viewed through this "dot perspective" is to understand what is contained in the voids between known points and to determine how the dots we don't have (unknowns) could be distributed in ways we do not understand. Our challenge is to present the alternatives and imprecision in a way that is useful for decision makers. If we do this right, we can still make decisive calls, but our customers will have a more realistic appreciation (and understanding) of the accuracy of our analysis and can account for the potential of error or surprise implicit in our judgments.

"Something" becomes an intelligence problem because it is unknown, but hypothetically ends up as both known and predictable. The biggest impact of dealing with unknowns is not on the IC itself but on the Community's customers. Sometimes we have operationalized our analytic and customer relationships well and account for intelligence unknowns. An example is how we operate aircraft in a hostile environment where we know the enemy has mobile SAMs, but we do not know their locations. Intelligence advises operators that the SAMs exist and to expect certain operating parameters for the threat, and then it advises that the locations are not known. Accordingly, the aircraft operators adjust their tactics. But how can this sort of informed, accustomed relationship between intelligence and aircraft operators be established across the *full spectrum* of analytic consumers?

There are at least three major components underscoring the importance of an unknown for intelligence analysts.

1) Unknowns Driving Collection

We have processes already in place, but there is room for improvement:

- telling our customers what we’re trying to find out;
- telling them what our expectations are for successfully finding something out;
- telling and portraying where we lack collection;
- letting customers know more clearly our uncertainty regarding source quality;
- continuing to develop alternative assessments of what we think we are seeing in collected data. (After all, deception is all about protecting truth by providing false “knowns.”)

In other words, giving our customers a clear view on our collection operations and expectations is important to helping them understand the intelligence product in the context of their needs.

2) Reporting and Assessing What We Don’t Know

Left to its natural tendencies, the IC will focus assessments and report on what it knows. There are some techniques that help:

- listing what we know;
- listing what we don’t know;
- listing what we think;
- being more comfortable with educated speculation, as long as we clearly identify it and offer multiple alternatives;
- assessing the potential impacts of the unknowns;
- assessing what could be wrong in our interpretation of the facts we have collected;
- providing more forthright evaluations of our sources to more people;
- making all of this consistently prominent (not just side boxes or sideline slides) in all assessments;
- using Red Teams for assessing what could be in the knowledge voids;
- emphasizing that admitting what we don’t know is an obligation—and good, professional practice—not an admission of failure.

If we execute this process in a clear-cut way, this transparency will support our ability to provide straightforward assessments. In fact, it will improve assessments because segregating “facts,” “thinks,” and “don’t knows” helps clarify for our analysts and our customers the basis of our judgments.

3) Threat Assessment And Warning

Our warning and threat assessment systems need to provide for:

- identification of collection voids and the threats potentially resident in these voids;

- an assessment of our ability to collect on key threat elements (such as terrorist cells) and the implication of these strengths or weaknesses;
- a disciplined methodology that accounts for collection voids in setting or explaining the threat level;
- an effective operational relationship with the Threat Warning Community that helps them establish postures or procedures based on the analytical assessment of the collection voids and unknowns identified.

Our best analysts already understand the significance and importance of “unknowns.” Our best intelligence products already reflect this. The biggest challenge is to support sophistication when we find it and to push it down and out across the analytic (and reporting) community. While we are emphasizing the art and science of analysis and directing energy on improvements, we must focus as well on accounting for the unknowns in our procedures and products.

Better Intelligence Community Organization

Since its founding in 1947, the IC has been structured organizationally to exploit individual agencies’ specialized know-how by maintaining their independence and prerogatives. Executive Order 12333 signed by President Reagan in the early 1980s codified IC agency independence by mandating that “competitive analysis” be the Community’s approach to developing national intelligence for decision makers. Competitive analysis allowed peer review of an agency’s products. It prevented one agency’s views from being represented as the best picture. Competitive analysis allowed agencies to comment on each other’s work without inhibition. It promoted healthy debate on the nature of the Threat. The problem with competitive analysis, however, can be that it works best when the problem set is well defined (such as the Soviet military threat to U.S. security during the Cold War) and when several analysts from different agencies can devote sufficient time to create the basis for a healthy debate. It does not work as well when the task before us is to identify new challenges posed by threats from new directions. It is less effective when there are fewer analysts available across the Community to engage in a robust debate. Competitive analysis can deliver lowest common denominator consensus assessments in the absence of a strong executive who appraises the quality of the answers developed during the competitive analysis process.

The Community has evolved into its current form of independent agencies based on a bottoms-up requirements-driven process as needs and technologies manifest themselves. As a result, the IC has taken on the attributes of a large conglomerate, with agency-unique sources and methods producing different product lines for a non-homogenous customer base. As with all conglomerates, the organizational challenge for the IC and its first DNI is improving performance. This improvement will occur by getting individual parts to reinforce each other to create a shared enterprise environment without diminishing opportunities for dissent, independent thinking, creativity or imagination. When the parts of the conglomerate are offered incentives for ownership of information delivered as agency-identifiable products, it creates an environment of competition that inhibits full sharing of information. If, however, rewards are based on the quality of the collaborative effort, overall IC performance improves without sacrificing the competency of each of the collaborating agencies.

If the IC is viewed as a conglomerate, then the new DNI should assess the governance and organizational structures of successful private sector conglomerates that could be employed by the IC. Examples include corporations such as General Electric, producing products from light bulbs to jet engines, and Time Warner, a company that sells a wide range of intellectual property in a variety of media in different market spaces.

Many successful private sector conglomerates, as well as the U.S. military, share a philosophy of centralized leadership and decentralized execution. Such leaders establish goals for the enterprise and expectations for how each individual unit will contribute to meeting these goals. Equally important, the conglomerate's officers have the means to enforce compliance with enterprise goals and expectations. Normally, management is decentralized for execution at the unit level. Important to the success of this management model in the IC will be organizational constructs that encourage both horizontal interactions across individual agency lines as well as vertical discourse between the DNI's senior staff and its counterparts at all of the IC agencies.

The competitive analysis organizational model, with its underlying linear extrapolative methodologies that the IC has used throughout the latter half of the 20th century, has supported the creation of stove-piped collection and production agencies. A feature of competitive analysis is to isolate external influences by other disciplines or agencies so as not to overly influence an individual agency's assessment. The IC created few organizational interfaces for horizontal or vertical communication prior to the completion of an agency's analysis.

Once confirmed, the new DNI can improve this situation without massive structural change by ensuring collaborative analysis. The DNI can enforce a shift from competitive to collaborative analysis by the questions asked about intelligence brought to his attention. Questions such as: What agencies were involved in producing this product? From where did the data it relies on come? What analytical techniques were used? Has a quality assurance check been run? The product's customer will have an immediate effect at the agency level of developing informal interfaces for sharing data and interpretations of what it could mean. The DNI should take steps to ensure that all analysts have thorough access to the same underlying data. In addition, the DNI's staff could look at how medical professionals share information to address difficult diagnostic situations or at techniques aircraft accident investigators use to determine the causes of accidents for applications that could be inserted into IC professional development curricula.

This preliminary list of actions would demonstrate the DNI's commitment to managing the IC as an enterprise rather than as a collection of individual holding companies, each with its own agenda. Most significant, by requiring the IC to move swiftly from competition to collaborative analysis as an organizing construct, the first DNI will be establishing authoritatively his intention to lead and manage the IC as an enterprise focused on insuring the national security of the United States.

Rebuilding Intelligence Research

The world is changing dramatically, creating many new intelligence challenges. Sources of information are exploding to include new National Technical Means, tactical, commercial and open sources. At the same time, the demographics of the analytic workforce also have changed dramatically. A flattening and then a precipitous decline beginning in 1993 followed the build up of the Reagan years. From the fall of the Berlin Wall until 9/11, the Community lost more than 23,000 positions. Since 9/11, the Community has been in an intensive rebuilding phase, resulting in a significant age and experience gap between entry level analysts and experienced staff. The confluence of the "greening" of the workforce, the proliferation of threats and the crescendo of data raise significant challenges to creating the integrated intelligence enterprise required for our national security.

Long-term research on intelligence problems has diminished alarmingly in some places. Intelligence research is the internal capacity and capability of the analytical staff to perform extended study of problems. A number of factors have contributed to the decline in this area, notably reduced manning levels. Fewer analysts have less time to read more traffic; still fewer can keep up with their part of increasingly complex targets of interest. Moreover, the emphasis on topical reporting has increased. When the enterprise recognizes and rewards the creation of articles for the President's Daily Brief and Senior Executive Intelligence Briefs, the creation of longer-range analyses suffers. Where once it was perhaps normal to expect one or two carefully researched papers per year, today's analyst has little opportunity for reflection, much less for longer-term research.

Entry-level analysts today bring a different skill set than previous generations. Critical thinking, logical decomposition and basic writing skills appear to receive less emphasis than in previous years. In contrast, Internet, multitasking and teamwork skills are often impressive. Nonetheless, analysts need more time in their daily schedules for extended studies and specific training to develop the necessary critical skills to perform classic, thorough research and analysis.

Sociologists have qualified significant differences between the generational characteristics of Boomers (1946-1954), Tweeners (1955-1963), Gen X (1964-1978) and Gen Y (1979-1999). These differences are compounded by a missing generation in the analyst workforce, from about ages 27 to 36 (1969-1978). Intelligence training has to deal with the transfer of knowledge from a dwindling cadre of experienced analysts to a growing cadre of younger analysts, who think and learn in different ways.

The archetypical analyst grew up in an era of vertically integrated systems focused on a monolithic target. Specialization was encouraged in specific domains like SIGINT collection or IMINT exploitation. Cross-system tipping, if it happened, was through informal and ad hoc means. The target, though dangerous, evolved slowly, with ample time to consider the implication of changes. Collection capacity grew dramatically, providing a surfeit of observations enabling sophisticated site models, doctrine insight, etc. An analyst had years to develop a feel for the target. While discipline-related individual study was fostered, collaboration, especially outside the domain, was an exception. Formal organizational structures arose, with specific chains of command.

Today's analyst faces an entirely different world.

- Threats are more ubiquitous and diverse.
- The collection input has exploded in volume, variety and velocity.
- Timelines are reduced, with non-symmetrical enemies able to launch offensives with little lead-time.
- Target boundaries blur as targets consort across functional areas.

Further, Gen X-Y analysts march to a different beat. They are:

- More team oriented and naturally collaborative.
- More likely to take initiative to reach out and across boundaries.
- Less sensitive to organizational constructs.
- IT-savvy and likely to build a Web version of the analyst shoebox when more capable solutions are not at hand.
- Fast learners, able to search and discover information adeptly.
- Less likely to reflect on the significance of data and communicating import ("telling the story").

The operational pace in today's analytical environment is hectic. OPTEMPO has increased dramatically. The rapid acceleration in hiring has not yet met the demands of the new threat environment. The fear of missing another 9/11 has taken "mission critical" to heightened levels of significance. Compounded by the absences caused by the large number of deployed military analysts, the pace puts a strain on every member of the analytic team. The constant demand is counter to the needs for both mentoring of other analysts and self-development. Important changes are required.

There is a need to enhance the formal training-mentoring program. A formal training and education program has long been a staple of the IC. There are numerous discipline-specific schools, and they are generally good at what they do. In addition, most agencies have some form of mentoring program that pairs new analysts with more seasoned veterans. No matter how well these programs might have worked in the past, we need to do better. Training curricula need to be coordinated across the community, with an eye toward enhancing horizontal integration and cross-discipline collaboration. The mentorship programs need to reinforce the responsibilities of mentors and to establish common measures of effectiveness. Rotational assignments are used effectively in industry; the IC should embrace them. Doing so would lead to more complex and rewarding mentoring relationships. A three-tiered model is used effectively at NSA: a peer-mentor young enough to relate to the view of the world of the employee being mentored; a long-term mentor who is a constant beyond the training period; and a domain mentor who is experienced in the current assignment area. The burdens of the mission need to be balanced against the strategic need for training and development to ensure that the "tyranny of the urgent" does not short-change the training needs.

The DNI should reestablish the importance of in-depth studies, including the ability to research in the native language of the primary subject. Now is the time, with the influx of new analysts, to reestablish the practice of creating study pieces once or twice a year and to emphasize language skills. The initial shortage of seasoned veterans to provide coaching in the area or in-depth research can be addressed in part by using recent retirees or faculty members from the intelligence schools. As the Community moves to the more integrated sharing environment for which the Intelligence Reform and Terrorism Prevention Act calls, these research papers will prove invaluable in providing answers to frequently asked questions as well as to questions that are not asked very often.

We must invest in critical technology components. The scale and diversity of the IC dwarf every analogy to which it has been compared. The IC is a microcosm of all the data in the world—a daunting environment. Immediately after 9/11, some pundits were quick to say that we needed "the mother of all databases" to help us "connect the dots." Both metaphors are inadequate. Rather than connecting dots, even unnumbered ones, the analogy is more akin to trying to solve a jigsaw puzzle by scooping into a river of pieces, most of which do not fit the puzzle. The creation of a database large enough to hold the river is beyond our capacities. Within reach, however, is a growing population of knowledge islands, instrumented to support a community of users focused on a specific mission. Many companies and universities are creating advanced technologies to support data integration, mediation, discovery, visualization, assessment and dissemination. While no single product, or even suite of products, provides the complete answer today, real progress is being made. Significantly these products are largely interoperable, given the rise of technologies such as Web services. In response to the Intelligence Reform and Terrorism Act's requirement for an Information Sharing Environment, the Community has an obligation to take advantage of these results.

The IC must also come to grips with the reality that unambiguous warning indicators have disappeared along with the Cold War. Ambiguous indicators often do not become clear until after an event has occurred. Our analytic methodology must forecast better by anticipating potential actions of our adversaries and aggressively seeking to confirm them, or, when possible, providing decision makers information they can use to preclude them. This process is active rather than passive, examines intentions as well as capabilities and is more inductive than deductive.

Even as the Community seeks to achieve needed changes in the scale of its operational capabilities, it should adopt an incremental approach to acquiring new capabilities for specific, hard problems. AFCEA has previously advocated a model akin to business-to-business concepts for integrating the multiple components of the IC ("National Security and Horizontal Integration, 2004"). We re-affirm that view, having noted the challenges faced by "big bang" programs in addressing pressing mission needs. The scale and complexity of the IC are simply too vast for an entirely integrated top-down approach to succeed. The World Wide Web would still be a dream if it had taken this approach. What can and will work is a common architecture in which can grow the continued federation of communities of interest, using the full range of data categorization techniques. Simple data base entity definitions, data tagging, taxonomies, ontology, guided navigation and other discovery techniques all have a role to play. Two requirements are paramount: one is the necessity to deal with legacy information that was collected before the data associations were known; the other is the ability to deal with emerging associations that traverse all previous clustering of data.

Achieving effective long-term intelligence research is an increasing challenge for the Community. Emerging solutions in knowledge transfer, communities of practice and others, coupled with a refocused training and mentoring program, offer hope that the challenge can be met.

Distributed Analysis

A clear imperative exists for distributed, networked analysis. In Iraq, U.S. forces are fighting against a highly decentralized enemy employing asymmetric tactics. The piece of HUMINT providing context for the COMINT that allows us to capture an insurgent demands that our analytical effort spans all intelligence disciplines and includes all of Iraq and its neighbors. In our echeloned organizational structure, the HUMINT may have come from a squad on the streets of Baghdad while the COMINT may have been gleaned from national means. Success is achieved only when we fuse and find meaning in disparate facts that have become separated by time, space or source.

On a larger scale, the Global War on Terrorism is just that—Global. The indicators of the 2001 attack on the World Trade Center go back at least as far as the failed attempt in 1993 and span many years of disciplined planning, preparation and training. Connecting those dots, finding all the right pieces of the puzzle, is a daunting—but not impossible—challenge. We won’t accomplish it with the status quo.

In our quest for creating distributed analysis, we face several obstacles, many self-imposed, and all surmountable. During the Cold War, the intelligence challenge was largely one of collection: finding out about forbidden targets in closed societies. As other authors have noted, collection is still important, but we are at risk of drowning in a massive volume of raw information. To make sense of that information—turning it into intelligence—we must have access to it. Contemporary approaches largely comprise filtering, or achieving data reduction within a single intelligence discipline, often resulting in product reports. The problem is that this filtering casts aside far too much information before it is analyzed. Filters are not sufficiently well informed and adjusted by further analysis. We believe it’s worth asking: Would distributed analysis have enabled us to focus on the 9/11 attackers conducting flight training in advance of their hijackings?

The cognitive "primacy effect" is a real challenge. It affects heavily how we interpret subsequent information. Like the inventory model of First In First Out (FIFO), it puts a premium on the analyst’s ability to formulate good hypotheses of what is probably happening, based on fusion of ambiguous bits and pieces. In other words, the greater the filtering, the smaller the fraction of information examined and the greater the chance of a skewed or misleading initial (and long lasting) hypothesis. WMD in Iraq is a likely example of this mental trap.

We must also overcome the problem of data ownership. While there are legitimate reasons to treat some information differently to protect sources and methods, far too much is not shared, often as a result of individual organizational interests

As previously discussed, in some cases "competitive analysis" has been distorted over time to become, instead, "competition." This can drive the preservation of stovepipes under the disguise of a "need-to-know." The key ingredient, as well as the enabler for effective competitive or collaborative analysis, is sharing of information with all competitive analysts, a process well known to peer-review-driven professions. Information sharing is in the eye of the beholder. Too many think it means only engineered connectivity to information (right permissions, tickets and tokens–sometimes granted only to the select few). This can lead to intellectual arrogance, elitism, groupthink and excessive weighting of information from sources "owned" by a specific agency. It precludes meaningful collaboration and distributed analysis. It precludes "tough competition" in favor of membership in competing elite clubs of special ticket holders. And, it precludes real "all source" fusion and squanders our potentially asymmetric information advantage. The new DNI should drive the Community forward by aggressively implementing the tenets of recent DCI guidance, making clear the risks of failing to do so.

We are also hamstrung by Cold War-era classification policies and procedures. We continue to protect sources and methods that are well known. In fact, they are often duplicated by commercial capabilities. We continue to demand a “need to know” when decentralized operations, chaos theory and the science of non-obvious relationships tell us that we cannot know in advance what information will be relevant and therefore needed. We are trapped in an “Alice in Wonderland” world in which we can’t know what we need to know—so we don’t! We are in a world where our national agencies possess an unparalleled picture of the global situation but can be blinded to the fights that are being conducted town-to-town and street-to-street in Iraq and Afghanistan. Meanwhile, the soldiers in harm’s way on those streets have exquisite local knowledge that can be gained only by being there, but they are ill equipped to contribute what they know to a shared database. They lack automated tools to fuse information and often cannot access other localized sources, much less theater and national assets.

Distributed analysis allows us to exploit our own asymmetric advantages against tough adversaries and tough analytical challenges. As it is sometimes described, our goal is to “link a million brains.” Automation is absolutely necessary to deal with an ever-increasing volume of information, but the most potent analytical weapon will always be a good analyst.

Distributed analysis cannot happen without universal access to data. That requires a network, and it requires enlightened policies that permit access granted by organizations that share raw data rather than finished products (which removes not only most of the data but also introduce bias and latency). It requires interoperability and data standards that facilitate efficient sharing, such as XML and PML tagging. Of equal importance, it requires collaborative tools that permit analysts to interact and pool their brainpower. We must be able to share raw data as a starting point, but we must also be able to conduct analytical processes synergistically and be able to share the output of that analysis.

An example of how this concept is being used is the U.S. Army Intelligence Center's concept of a commander's running estimate (CRE). While current technology and procedures are capable of a reasonably effective common operating picture (COP), the center's goal is to deliver to decision-makers a dynamic, graphic CRE that incorporates analysis and thus becomes predictive. Rather than just present the most complete depiction of the present, it will deliver an intuitive representation of the future, or multiple futures; it will facilitate war-gaming; and it will include not only intelligence but also all of the battlefield functional areas, including operations, logistics and administration. This fused picture promises better, faster, more holistic decisions.

Another example can be found at the Army INSCOM's Information Dominance Center (IDC). The center employs technologies to achieve distributed analysis. It has established the network and universal access to data that links the main IDC at Fort Belvoir with IDC extensions at each of the theater commands and ultimately to a host of intelligence collectors and consumers. Via a data mediation layer and data tagging, vast stores of data can be shared, fused and analyzed. This approach allows analysts to search, visualize and analyze disparate information rapidly to determine relationships, relevance, accuracy and significance along tactically useful timelines.

Technology alone will not deliver distributed analysis or its desired product—an enhanced state of shared situational awareness across the IC. We must overcome barriers of culture and mindset. In addition to problems created by data ownership, we must overcome the perception that an analyst is not fully engaged in the fight unless he or she is physically present. Rather, the optimal solution is a virtually linked team of analysts and operators who can achieve far more than can be accomplished by physical collocation. Participants in this system must trust intelligence that may be disassociated from its source, perhaps contributed by a participant a hemisphere away, but that may provide a unique contribution to the shared understanding of important problems.

Distributed analysis is not really optional. The Community already has the world's best analysts. Our challenge is to synergize their efforts, an imperative based on the nature of the contemporary threat.

Transforming Analysis

In the wake of the 9/11 Commission report and the passage of the Intelligence Reform and Terrorism Prevention Act of 2004, the IC is again examining ways in which a truly national intelligence capability can be built, one capable of meeting our nation's needs in a complex, dynamic and challenging world. Much of the Community's examination is focused on organizational and resource questions. We propose assessing the intelligence methodology as a *driver* for organizational reform.

The 9/11 Commission's injunction to "connect the dots" highlights the need to find and recognize patterns of activity (or meaningful intelligence) comprised of data from disparate sources, collected by a variety of means and subjected to a myriad of analytic processes. The Commission and the Reform Act point to a variety of capabilities needed to build interoperable intelligence capabilities. In establishing a DNI, the Act provides the foundation for Community-level management of resources leading to integrated intelligence collection, analysis and products. Nonetheless, the bulk of actions undertaken or under consideration as a result of the Commission and the Act relate to organizational reform and more integrated resource management. An underlying need exists to examine fundamental concepts that govern the relationships among collection, analysis and dissemination—and other components of the traditional intelligence cycle. Absent such an examination, even the most effective resource management by the DNI will not lead to better production of intelligence using the means and approaches the Community already has available. Reason exists to doubt the extent to which timelier, comprehensive and meaningful intelligence would be provided to the national security community.

Analysis throughout the Community, while often effective, is hobbled overall by resource management approaches that separate collection from analysis and analysis from dissemination. Although the term "mission management" is part of the intelligence lexicon, it frequently refers generally to "collection management" in which intelligence requirements drive the tasking of collection resources. As a result, the injunction given by some intelligence seniors to move from "analyzing what we collect" to "analyzing what *to* collect" founders on the lack of real-time management tools beyond those used to manage the front end (collection) of intelligence activities.

This focus on "collection" rather than "mission" management leaves the IC in a situation analogous to a manufacturer more focused on "inputs" than on "manufacturing." Consider briefly the resulting plight of an automobile manufacturer that uses consumer demand for products and features to decide on the acquisition of raw materials, leaving decisions on how to allocate and manage internal manufacturing resources as derivative of the availability of raw materials. An even more extreme example would be a decision to base both decisions on what product to produce and on the allocation and management of production resources on the availability of raw material. In the intelligence context, such approaches are not uncommon. Customer requirements drive collection, leaving the allocation and management of analytic and other resources as derivative of the raw intelligence data collected in response to consumer needs. In some cases, the availability of data may even define what is done with the rest of the intelligence process *and* the product made available to consumers. In the case of a manufacturer, a more comprehensive mission management approach might uncover stockpiles of raw material already available to the company, and it might reallocate existing manufacturing processes. It might also consider and manage competing requirements in the context of all of its productive capacity, “trading” requirements and resources dynamically. It would use an enterprise view of workflows to manage the totality of its resources.

The IC has experimented with mission management approaches based on the visibility, allocation and management of resources from collection through dissemination. An even more serious commitment is necessary. Programs such as IC-MAP, designed to give consumers a “one-stop” portal for their needs and visibility into collection strategies applied on behalf of their needs, are supported inconsistently across the community, even as individual “INTs” maintain separate collection, analysis and dissemination infrastructures. Further, the uneven acceptance of enterprise approaches to intelligence infrastructures, in which a variety of missions share data and achieve operational scale across a common infrastructure, makes difficult the implementation of common and comprehensive mission management. As a result, data (relating to intelligence target activity) and “metadata” describing intelligence targets (for example their operational concepts, infrastructures, relationships) are shared inadequately. Little wonder that “connecting the dots” or finding the correct puzzle pieces remains difficult, given the relative poverty of tools to manage in common the resources that collect, process, analyze and produce information about the “dots.”

Within the various “INTs” themselves, a variety of organizational models impede progress toward effective intelligence support to consumers. For example, data collection is organized around collection mode. The IMINT, MASINT and SIGINT communities are organized at the top level around specific portions of the electromagnetic spectrum employed to gather raw data. Analysis is organized around intelligence subjects or issues, while dissemination is organized in some cases around the consumers supported in specific relationships. “Impedance mismatches” in the management of resources organized in these three orthogonal models are an inevitable result. Although it is beyond the scope of this paper to recommend a specific organizational model for intelligence, a brief look at industry offers some interesting clues.

Large manufacturers are organized around consumer types (e.g., households, young couples, institutions). They manage common infrastructures for purchasing things such as raw materials and production in support of specific consumer needs. In doing so, they have built infrastructures on which customized workflows can be employed in support of dynamic consumer requirements. Such organizations have become truly “customer-driven,” a phrase heard often in the IC.

There are inevitable costs to moving toward comprehensive analysis. Existing, separate infrastructures, built around data access types, intelligence subjects and consumer relationships, represent significant sunk costs. Recurring costs associated with their continued operation have likely been programmed for future years. More important, intelligence professionals with valuable expertise and accomplished track records have invested themselves in the management of target-, subject-, customer- and “int-” specific infrastructures.

The establishment of a DNI represents a powerful opportunity to examine and help the components of the IC create resource management and organizational concepts more attuned to an international security environment in which collection modes, subjects of intelligence interest and consumers are intermingled. Within the mandate of the Intelligence Reform and Terrorism Prevention Act lies flexibility to encourage reform internal to each agency, both in terms of organizational concept and resource and workflow management. Although the Act constrains the DNI within the context of certain joint responsibilities (exercised, for example with the Secretary of Defense), it provides the DNI with sufficient budget, acquisition and operational authority to cause incremental, but important, changes. Although the Act specifies the appointment of a Principal Deputy DNI and other Deputy DNIs, it leaves to the DNI's discretion the composition of the Deputy DNI cadre. That composition should certainly take into account the opportunity afforded by the Act to build organizational and resource management concepts that create a truly integrated national intelligence capability.

In the end, intelligence reform goes beyond organizational "boxology" or "connecting the dots." Both of these are artifacts of a greater imperative: the need to build a national intelligence capability in which resources are managed dynamically in response to a changing security environment and in which the totality of the intelligence cycle is managed as a whole to gain the coherent comprehensive intelligence picture our decision makers need. The means to accomplish these goals are within our grasp.

Putting the Analyst Back In Analysis: Human System Effectiveness

Having examined various approaches to the future of analysis, we believe there is reason for the Community's leadership to adopt an analyst-centric framework to confront emerging intelligence challenges in order to "put the analyst back in analysis." A focus on human-systems effectiveness is essential to the transformation of the nation's intelligence capabilities in order to reinforce the role of the intelligence analyst as the essential component of the triad of organization, process and technology. Great effort is going into technology to assist the analyst in acquiring, processing and accessing information. Organizational restructuring seems constant. Systems engineers are mapping out new business processes and designing larger and faster conduits for improved information flows. Unfortunately, algorithms being developed are challenged in providing context to data streams. These algorithms cannot readily provide meaning to the data. Only the analyst (whether located in a national agency or in a tactical command post) can provide that meaning through the human cognitive process. Hence, a need exists to make human-systems effectiveness an integrating concept of the future intelligence enterprise. This is vital if we expect our intelligence analysts to understand the dynamic landscape of international events and threats to the nation, to apply critical thinking to complex and ambiguous information and to translate both into timely intelligence useful to the war fighter and to the policymaker.

In addressing the challenges described in this series of papers, the IC has often emphasized information technology-enabled process changes for horizontal integration as well as prioritized funding for development of new tools and intelligence gathering systems to address its most difficult problems. However, this approach obscures the underlying reality that intelligence analysis is still not deterministic and is still just as reliant (if not more so) on human judgment as on technical processing. There is a danger that an all-consuming focus on technology can lead to piecemeal investments that may not address the totality of an issue or its full analytic context. The IC is a knowledge-based enterprise where speed and processing capability are important, but content and accuracy are more so. Before the IC is overwhelmed by the promise of "net-centricity," or "data-centricity," it needs to consider "human-centricity," placing the analyst at the center of the future of analysis.

The IC needs to embrace human-centered design with the analyst considered early in research efforts and in the development of new tools and system requirements. This approach will lead to a future integrated information environment that matches the way users perceive, think and act. New display interfaces should permit an intuitive portrayal of multi-source data in a way that will aid real-time management of tasked information. Information displays should become multi-sensory and three-dimensional, moving beyond visualization to "perceptualization." Intelligent agents should be able to perform tasks proactively on behalf of the user, allowing system configuration based on the needs and skill of the user/analyst.

Understanding the theoretical foundations of analysis, including cognitive models, is important to improving intelligence. Pioneer thinkers such as Richard Heurer have argued that one key to better analysis is not more and better information but rather understanding the limitations in the inherent mental models used by analysts. Much innovative research is currently focused on how analysts perceive and use information. Enhanced knowledge of the linkages of the different physical senses to information portrayal and analyst brain function is aiding in the development of smart agents to assist analysts. The Defense Advanced Research Projects Agency (DARPA) and the Advanced Research and Development Activity (ARDA) both have interesting projects in this area. The Air Force Research Laboratory is looking at the timing of visual information appearing before an analyst (or operational planner or pilot) to see how data flows can best be managed to maximize cognition and minimize error. More significantly, a number of universities as well as industry are conducting research into virtual environments that bring in other senses to assist analysts and users, including immersive 3D displays and new ways of interacting with the data. Such research, along with an analyst-centric approach, will form the basis of other, longer term work to help develop better analytic tools, better tradecraft that recognizes individual analyst strengths and better indicators of analysts' adaptability to new training methods and evolving analytic tradecraft. Continued emphasis is needed in this area as it provides the starting point to determine analyst needs for the future of analysis.

Building on an understanding of analyst cognitive processes and continuing advances in technology can aid analyst productivity. Displays and interfaces that are context-appropriate and intuitive enable more rapid understanding and resolution of events. In areas such as time sensitive targeting, a real need exists to perceive and comprehend critical information with less data clutter. Techniques such as synthetically pacing information flow can lead to near real-time adaptive interfaces. For more complex and longer-term problems, intelligent agents can perform tasks on behalf of the user and allow portrayal of information according to the preference of the individual analyst. They can also permit re-creation of the analytic method used for more difficult analysis (such as from advanced geospatial intelligence, or AGI or MASINT) or for collaborative analysis. One approach cited in the first AFCEA White Paper was to look for "commercially available …tools [that] can help an analyst discern and understand obscure linkages between individuals, activities and methods of operations." Turning to commercial sources for unique intelligence problems can have its drawbacks; however. It is not always clear if commercial hardware and software tools have been developed with analyst cognitive processes in mind or if they allow alterations for user preferences and tradecraft requirements. Analyst considerations should be involved at all stages of development rather than as an afterthought as is too often the case on many tools and interfaces in use (or disuse) on analyst computer desktops today.

Other organizations have taken user-centered requirements to heart. The Army has created a Soldier System Center as well as an acquisition office (PEO Soldier) to champion soldier needs, while the Air Force uses the Air Force Research Lab to bring human effectiveness into its development and engineering work. In integrating human effectiveness into systems development, the Community should avoid the use of a deterministic "interface standards manual," that specifies (for example) screen luminosity. The Community should also bring the analyst into the development process early and frequently. Within the Community, systems development retains an overwhelming engineering focus that values efficiency, flow rates and cost concerns. The result is systems designed by engineers and built for hypothetical users who may not exist. A more contemporary, iterative development approach, in which users are part of the development team throughout the development process, makes more sense. Such an approach would also aid in the adoption of commercial technologies, ensuring that such technologies are employed only after their usability by intelligence analysts has been established. Overall, the IC as a whole would benefit from a human-systems effectiveness (HSE) program as an integral part of systems development requirements and evaluation criteria.

As pointed out above in "Rebuilding Intelligence Research," the current analyst workforce is ageing. As it retires, new generational challenges are developing. Some see older generations as "digital immigrants" set in their ways, not fully comfortable with changing technology and tradecraft. Newer generations, such as Millennials (those born after 1980), have different expectations about workplace and career. They are "digital natives," willing and able to adapt and use technology in new ways and comfortable with change. Millenials prefer to work in unstructured, technologically advanced organizations. Yet, we often bring them into a restrictive work environment, with desktop systems less advanced (and less tailorable) than what they have at home, and restrict desktop Internet access (despite the fact it is a major source of information).

While some restrictions exist for valid system configuration or security reasons, they lead to a problem of expectations. If promised advanced tools, tradecraft and processes are not soon available, the contemporary analyst will either grow bored and frustrated with older technology (with a detrimental effect on the quality of analysis) or may decide to seek something more stimulating outside of the national security environment. Mixing dissimilar generations together in work teams creates differences in work management expectations (frequent or infrequent meetings, flexible hours or standard hours) and work habits. New workplace policy and flexibility are needed to recognize the strength of different generations of analysts, to retain skilled senior analysts for their experience and knowledge and to welcome new analysts for their creativity and flexibility. At the same time, we should not expect a new analyst to enter the intelligence field after college and stay in the same agency and career field for the next 35 years. Broadening and experience in other fields are needed, or movement into the private sector and then back into government with portable benefits packages should become easier. Addressing these issues though future workforce planning is an integral part of the human-systems effectiveness approach to the future of analysis.

One area also needing a new approach is the recruitment process to find the right type of intelligence analyst of the future. Some suggest the skills needed by analysts are those of artists or musicians, more comfortable in an unstructured environment where they are unconstrained in their ability to approach a problem in novel ways. Currently we hire analysts with very little cognitive testing; put them through standardized training; and wonder why so much attrition occurs before we get a fully capable analyst some 18-24 months later. One approach being explored by Georgetown University and MITRE is to test spatial skills in imagery analyst applicants to see what traits are innate and what traits are gained after years of training and practice. Exploring this area of what psychologists call nature versus nurture can give the Community an idea regarding how to focus training and how to hire analysts with the right skill sets. Other selection criteria to consider could focus on personality and motivation for matching recruits with appropriate types of work. Hiring these "correct" analysts could potentially reduce the large attrition rate of new analysts.

Finally, the intelligence analyst needs an updated training and promotion system. Broadened skill sets and multi-intelligence teams are the new paradigm for analysis. The second AFCEA White Paper discussed creation of a National Intelligence Workforce and behavioral incentives modeled on joint billet requirements for military promotion in the Goldwater-Nichols Act. With this in mind, creating common foundational level training for all analysts upon initial entry with the intelligence services will create a common baseline, a broader vision of analysis and a chance to make contacts that will be useful throughout a career. Rotational assignments, perhaps required for promotion to senior levels, are also needed. This will broaden the common baseline and understanding of the entire intelligence enterprise.

Clearly, better technology, improved process, revised tradecraft and streamlined organization represent only part of the solution for improving future analytic capabilities. In the end, analysis remains an art and relies on the intuitive ability of the human mind. The analyst is the key part of the enterprise. Technology is a tool to help analysts think better. It is not a substitute for thinking. As such, tools and technology can never be a substitute for analysis, but they should assist analysts in digesting and assessing information. Systems engineers need to recognize analyst requirements as an equally important component of system design. Similarly, organizational structure and policy should adapt to the changing generational strengths of intelligence analysts and reward critical thinking. Adopting a human-systems effectiveness approach to the future of analysis can enable the analyst and can produce better results for the nation.

Summary

The contributions offered in this third AFCEA White Paper represent a range of recommendations worthy of the Community's serious consideration. Some of the most salient recommendations include:

- Concerted focus on unknowns, that is, real emphasis on understanding the gaps in our knowledge, giving decision makers analytic options that encompass these unknowns, rather than extrapolate around them.
- Consideration for the components comprising the IC of organizational models used elsewhere and particularly organizational models adapted from the private sector.
- An approach to rebuilding the nation's capacity for sustained intelligence research, based on organizational and other models pertinent to the generation of analysts present in and entering the IC.
- Stronger efforts to build the means for distributed analysis, including operational and organizational concepts that capture the benefits of distributed analysis across a far-flung IC.
- The need to transform intelligence by creating mission management based on the analysis of the entirety of the intelligence cycle rather than on opportunities offered by specific collection means.
- An approach to organizing IC components in a consistent fashion rather than on organizational principles specific to collection, analysis and dissemination.
- New analytic approaches that reflect recent advances in the ways in which human beings interact with the information with which they are presented.

Together, these recommendations describe approaches to intelligence analysis relevant to the complex national security environment the nation faces today and will face in the future. Complex questions, involving transnational intelligence targets, require an integrated IC equipped with new analytic approaches, a stronger approach to analytic organization, mission management focused on the entirety of the intelligence process, and a renewed investment in the research needed to improve our understanding of the most challenging analytic problems.

The AFCEA Intelligence Committee knows these challenges are tough. We know, too that our nation can meet them. We must, and we will.