Aerospace Ground Equipment craftsman remains vigilant over 761 pieces of equipment for MQ-1 Predator and MQ-9 Reaper unmanned aerial vehicles (U.S. Air Force/Christian Clausen)

Activity-Based Intelligence

Revolutionizing Military Intelligence Analysis

By Chandler P. Atwood

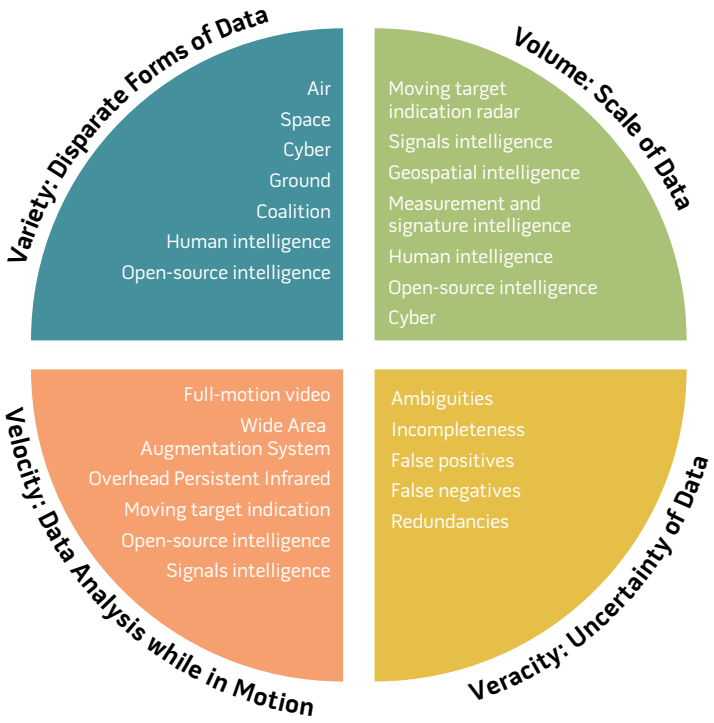
Information-age technology is advancing at a stunning pace, yielding increasingly complex information architectures, data accessibility, and knowledge management—all of which have created the conditions for a leap in intelligence processes," stated Lieutenant General Robert Otto, the Air Force Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance (ISR).[1] The vast amount of information that the Intelligence Community (IC) collects demands a transformation in the way the Department of Defense (DOD) intelligence enterprise processes, organizes, and presents data. The enterprise must embrace the opportunities inherent to big data while also driving toward a unified strategy with the IC. The primary strategy thus far has been acquisition based, looking to industry and research and development organizations to provide the next best tool and software, rather than addressing the more existential requirement of advancing analytical tradecraft and transforming antiquated intelligence analysis and processing methods.

In our current diffuse and multipolar threat environment, the DOD intelligence enterprise faces the daunting task of discerning abnormal and/or

Lieutenant Colonel Chandler P. Atwood, USAF, is Chief of the Commander's Action Group for the Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance. He was previously a National Defense Fellow at The Washington Institute for Near East Policy and Squadron Director of Operations at the National Air and Space Intelligence Center.

significant activities from normal patterns of activities. To truly revolutionize and fundamentally change from an individual exploitation process to analysis-based tradecraft, the enterprise needs to harness the potential of big data, replacing the methodology of individually exploited pieces of data with an activity-based analysis approach, known as Activity-Based Intelligence (ABI). Use of the ABI methodology will enable our intelligence analysts to focus on hard problems with critical timelines as well as normal day-to-day production activities across the spectrum of conflict. This methodology will aid in the development and understanding of patterns of life, which in turn will enable analysts to differentiate abnormal from normal activities as well as potentially defining a "new normal." Furthermore, the sharp incline in the amount of data, recent information technology (IT) advances, and the ABI methodology impel significant changes within the traditional DOD intelligence production model of PCPAD (planning and direction, collection, processing and exploitation, analysis and production, and dissemination).

Figure 1. The Four Vs of Big Data



Big Data: A Problem or Opportunity?

Today's IC faces the data challenges of the "four Vs" with persistent sensors soaking the battlespace: *variety, volume, velocity*, and *veracity*. The DOD intelligence enterprise processing, exploitation, and dissemination (PED) systems and analysts cannot keep pace with the four Vs inherent in big data or continue to mitigate the tendency of each organizational entity to build stovepiped systems with poor interoperability overall.[2] The IC has dealt with data volume and velocity issues for decades, but the challenge has more recently expanded to include the full complexity of big data with variety and veracity added to the equation as illustrated in figure 1.

Even today in Afghanistan where ISR forces have been redundantly layered for years, the creation of a timely, coherent picture gained from integrated, multi-source intelligence data is a rarity. For instance, U.S. and North Atlantic Treaty Organization forces in Afghanistan have suffered losses when they were surprised by an unexpected larger insurgent force not detected and relayed in time even when there were ever-present ISR assets operating in a permissible environment.[3] This assertion still stands true today and portends an enduring DOD intelligence enterprise challenge of integrating disparate datasets into a clear picture for warfighters and their commanders across all types of battlespaces. Whether we reflect over the last 13 years operating in a permissive environment or look to the future in a potentially highly contested battlespace, DOD intelligence organizations will operate in domains in which all four Vs of data combine to create the big data conundrum.

Most DOD intelligence enterprise analysts contend that "drowning in data" leaves our intelligence organizations afflicted with overstimulation and overwhelmed with man-hour intensive PED. Specifically, the DOD Joint Distributed Common Ground System (DCGS) enterprise fits this paradigm and has yet to reach its full potential of networking and integrating the entire spectrum of national and tactical intelligence due to a preoccupation with data exploitation. DCGS is a system with a laser focus on single-source, quick-look reporting. It does not provide larger discovery from the integration of multiple intelligence (multi-INT) disciplines and sources.

Since 2003, the Air Force DCGS and the greater DOD intelligence enterprise have seen a steep growth in the number of sensors with multiple exponential increases in the data each produces, as well as the multiple forms of data formats they must process and exploit. For instance, we started this era with a strong and growing dependence on a narrow field-of-view full-motion video (FMV) MQ-1 Predator observing a 0.1 x 0.1 kilometer (km) "soda straw" spot on the ground. Today our DCGS core sites focus on processing, exploiting, and disseminating intelligence from dozens of MQ-1 combat air patrols while also absorbing increased data from newer sensors with a much larger target area coverage. In the future, wide area airborne surveillance programs of record will have a sensor coverage area of an enormous 30 x 30 km. These advances in motion video coupled with the expansion of sensor

coverage across the spectral bands, such as the data intensive hyperspectral sensors, and the burgeoning light detection and ranging sensors drive a significantly greater data problem concerning the four Vs. The list goes on, with increasing signals intelligence (SIGINT) sensors and moving target indicator (MTI) sensors as well as the growing integration of overhead persistent infrared (OPIR) data and nontraditional measurement and signatures (MASINT) sensors into the IC enterprise. This ever-expanding list of data generators leaves the ISR operators in a state of near paralysis and the training shops and leadership saying, "enough is enough."[4] Today's focus on single-source exploitation in an environment of multisource data availability clearly hinders analysts from understanding and conveying the overall meaning of the integrated results.

In today's dynamic and complex battlespace, the DOD intelligence enterprise requires near simultaneous access to and analysis of data from a multitude of sources and disciplines—thereby embracing big data. These integrated disciplines should include at a minimum SIGINT, human intelligence (HUMINT), geospatial intelligence (GEOINT), MASINT, and even open source intelligence (OSINT) to understand the problem and provide actionable intelligence to warfighters. Today's analysts tend to develop an expertise in only one or two of these disciplines, resulting in their inability to understand and convey the overall meaning of the integrated results potentially obtainable from all data.

In spite of big data overwhelming our existing ISR exploitation capabilities, there are indications that change is starting to occur. The increase in sensors and resulting vast amounts of disparate data coupled with the increasing capabilities of IT systems to handle the deluge are transforming intelligence analysis. The traditional process of stitching together sparse data to derive conclusions is now evolving to a process of extracting conclusions from aggregation and distillation of big data.[5] Although IT solutions will enable our analytical shift, the largest impact will come from replacing the methodology of individually exploited pieces of data with Activity-Based Intelligence. ABI is a high-quality methodology for maximizing the value we can derive from big data, making new discoveries about adversary patterns and networks, yielding context, and therefore also providing greater understanding.[6] The information age now brings the potential for technological improvements to harness big data in such a way that true ABI methodology can indeed become a reality.

Activity-Based Intelligence

Activity-Based Intelligence has already been defined in many different ways, and after many months of debate, a codified and agreed-upon definition, based on Under Secretary of Defense for Intelligence guidance, finally exists: "ABI is a multi-INT approach to activity and transactional data analysis to resolve unknowns, develop object and network knowledge, and drive collection."[7] The following paraphrasing may resonate more with DOD ISR professionals, enabling a better understanding of ABI, though not intending to replace or circumvent the established definition:

ABI is an analysis methodology which rapidly integrates data from multiple INTs and sources around the interactions of people, events and activities, in order to discover relevant patterns, determine and identify change, and characterize those patterns to drive collection and create decision advantage.[8]

ABI is an inherently multi-INT methodology that invokes a transformational approach to data processing and analysis. The methodology uses a large volume of data from a variety of intelligence sources to enable data correlations that, among other things, drive discovery of weak signatures and patterns in a noisy data environment. This methodology will fill critical gaps in single-source data PED processes. It will also help resolve unknowns through the process of correlating activity data with information about the attributes, relationships, and behaviors of known and unknown objects in ways that cannot be done today without proper automation. By accumulating the multi-INT data on individual activities, an ABI analyst can correlate activities, detect anomalies, and discover links between objects. The derived object and network knowledge will enable the discovery of new facilities, links and nodes, and patterns of activity. An ABI analyst correlating activities and resolving objects will enable real-time tipping and cueing of sensors, thereby driving collection, again, in ways that cannot be done today.[9]

Methodology in Action

The confluence of four Vs in big data requires a significantly different way of handling the task(s) that traditional intelligence methodologies cannot support. For instance, the Intelligence Community reportedly had pieces of information that provided indicators of the impending August 21, 2013, chemical weapons (CW) attack in Syria, but seemingly failed to process and integrate the information in time to portend such an attack. According to a White House Press Secretary official report, "In the three days prior to the attack, we collected streams of HUMINT, SIGINT and GEOINT that reveal regime activities that we assess were associated with preparations for a chemical weapons attack."[10] This reported shortfall raises troublesome questions for the analytical integration capabilities of the IC and provides a hypothetical backdrop from which to develop an ABI tradecraft workflow template applying its four pillars and main enablers.[11]

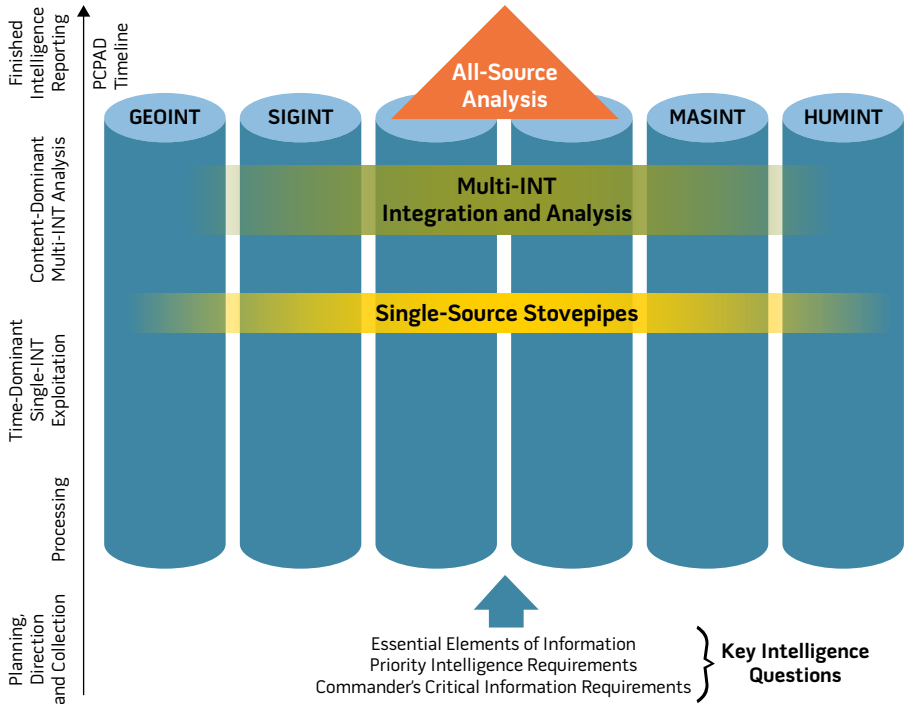
Perhaps the individual agencies had the data 3 days prior but failed to (or were unable to) integrate all the data from their respective data streams in order to first derive understanding and then to identify key indicators of abnormal activity in a way that would lead to a credible, defendable conclusion. Conceivably, the data associated with the individual intelligence components only made sense after the attack, when the events were manually retraced and integrated across the other data sources through a manpower extensive post-event reconstruction.

The ABI methodology will revolutionize the analytic processes applied to situations like this example in a way that will enable automated real-time correlation of data and information from current collections as well as through archived data sources. These data correlations can establish baseline understanding of the information, historic trends of activity, and provide identification of anomalies. When in action, the ABI methodology has four, not necessarily sequential, pillars: georeference to discover, integrate before exploitation, data (sensor) neutrality, and sequence neutrality.[12]

The absolute first step in the ABI methodology must be *georeference to discover*. All data sources should be spatially and temporally indexed at the time of collection rather than treated as an afterthought or last step in the analytic process as often accomplished today across the IC, if possible. ABI depends on a variety of multi-INT data that need to be integrated to fill holes in sparse single-source datasets. To mitigate gaps in single-source data, all of the collected data must be "georeferenced" to a specific point in space and time.[13] Only then will an ABI analyst be able to correlate, integrate, and cluster the multi-INT data around a "spot of interest," enabling the discovery of entities, activities, transactions, and begin to relate them.[14] Having preconditioned data, with explicit spatial and temporal aspects, allows the ABI analysts to spend more time applying contextual knowledge to the problem set, focusing their analysis.

Using Syria's use of chemical weapons as a backdrop, what if regime personnel were observed operating in an area used to prepare chemical weapons in the days leading up to the attack? Hypothetically, we could call this an analysis failure where the IC had the indications but did not integrate and make sense of the incoming multi-INT data fast enough. Imagine instead HUMINT and other data sources not fully used in the analysis had been georeferenced and temporally tagged at collection, enabling an ABI analyst to retrieve and integrate the sources through an interactive spatial application tool.[15] The ABI product then becomes a relationship "map" of the objects and entities and their transactions, such as those activities surrounding preparatory CW attack efforts. Even in contested battlespaces, where data sources are sparse, it is only through georeferencing all the available multi-INT data that the ABI analysts can begin their workflow.

Figure 2. Traditional and Current PCPAD Intelligence Process

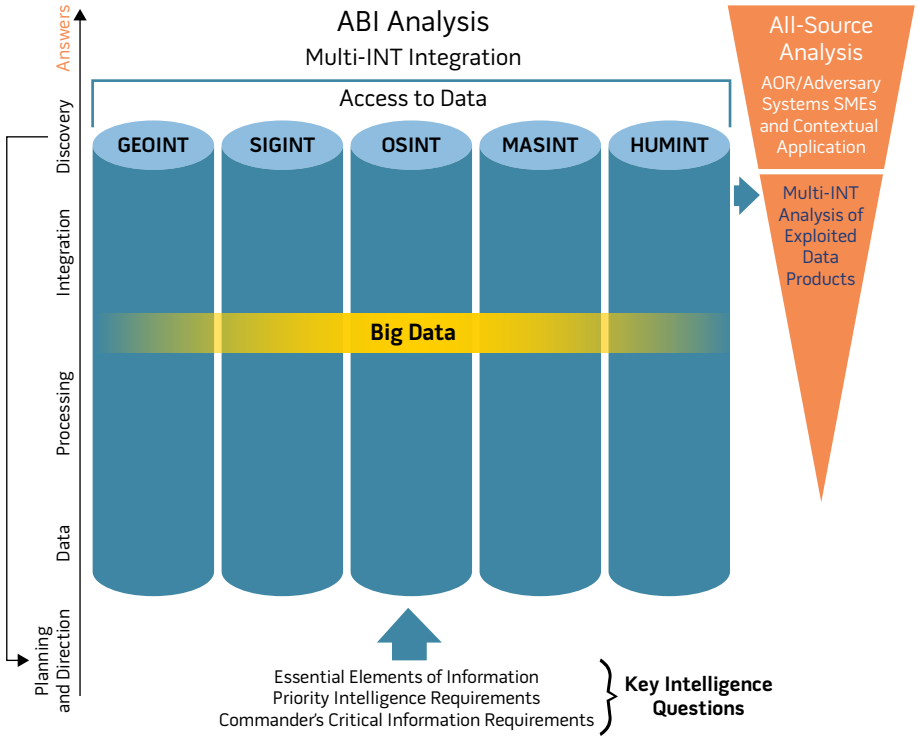


After georeferencing the collected data within the ABI context, it will be *integrated before exploitation*. Georeferenced data are associated at the earliest integration point, before an analyst conducts detailed exploitation and analysis, not at the end of the production process. The ABI methodology looks for relationships at the earliest point of consumption, applying context earlier than in the classic intelligence process. That process, codified in joint doctrine as a production model of PCPAD, integrates exploited and analyzed single-source information at the end of the process.[16] When executed, the PCPAD model narrowly focuses on exploiting the stovepiped data first and then passing to a multi-INT or all-source analyst to integrate the different pieces of exploited data as depicted in figure 2.

Still, much of the IC continues to be mired in a linear process that relies too heavily on a preset targeted collection strategy as well as an independent single-source PED and analysis process to address intelligence gaps. Yet by embracing the ABI methodology, the IC can overcome profound yet surmountable challenges of transforming this antiquated intelligence process and the related analytic tradecraft into one best suited for success in today's data-congested enterprise.

During execution, the PCPAD model narrowly focuses on a linear approach to pushing data, typically single-sourced, to address an intelligence gap driven by causation, like Syria's CW example. In this traditional method, some information may have been inadvertently discounted during the stovepiped exploitation process. In some cases, the relevancy of the information only develops significance when associated and integrated with another data source at the time of exploitation. The ABI methodology will provide the means of avoiding the trap of viewing data from a single source or multiple sources of the same discipline and making what may

Figure 3. How ABI Transforms the Traditional Intelligence Process



well prove to be inaccurate or incomplete value judgments before understanding the full picture.

In so doing, the ABI methodology enables analysts to sift through large volumes and varieties of data to see how the data overlap and intersect, identifying associations and enabling significant events to rise above the noise of data triage. For instance, in our previous CW example, let us now presume a HUMINT or SIGINT tip, not "finished intelligence" reporting, has been intercepted indicating that the use of CW had been ordered. This is information that could have been integrated earlier in the intelligence production process. A GEOINT analyst routinely observing imagery may have not seen abnormal activity days leading up to the attack. However, if the HUMINT or SIGINT tip had been known by the GEOINT analyst at the time of imagery exploitation, then what was potentially disregarded as insignificant activity may have been associated with preparatory CW operations and identified as such.

As depicted in figure 3, this potential ABI-derived discovery would then drive additional analysis including the time-dominant exploitation requirement of the GEOINT, SIGINT, and any additional INT data pertaining to that area. In this case, the time-dominant exploitation of the HUMINT or SIGINT provides the GEOINT analyst with enough insight to focus his exploitation efforts on a specific area of the imagery, potentially reducing exploitation resources. Assuming limited information is available to corroborate potentially anomalous activity, a dynamic re-tasking of sensors could be conducted, driving real-time collection. After the ABI analyst commingles the various pieces of data and identifies key pieces, exploitation begins to occur within each INT, providing the results to the multi-INT analysts to conduct integration of the exploited information and address the intelligence questions as the process continues to add additional information. Finally, an all-source analyst may receive the multi-INT integrated information to provide additional context and subject matter expertise to this ABI methodology discovered intelligence of preparatory CW operations.

In addition to PCPAD's inherent inflexibility to integrate single INT sources earlier in the process, it relies too heavily on an antiquated preset targeted collection strategy against known adversary targets. The PCPAD premise of targeted collection is highly reliant on known and distinguishable signatures supported with doctrinally aligned tactics, techniques, and procedures (TTPs) to be effective against such threats. The post–Cold War's diffuse and complex threat environment displays inherently nonstate threats, fleeting signatures, and minimally supporting doctrine from which to focus PCPAD's target-based collection strategy. To transform the current paradigm from a deliberate fixed target focus requires a revised model.

The ABI methodology does not have a traditional target-centric approach to analysis, like observing specific CW stockpiles and production facilities on a daily basis. Using the *integrate before exploit* ABI pillar, the analyst is informed by the commingled data, allowing him to search for observables and to potentially discover a threat signature or indicator that was not discernable in the PCPAD paradigm. An ABI analyst integrating a variety of disparate datasets in this fashion may have provided the activity linkage leading up to Syria's CW attack well before the intelligence process reached the all-source analyst.

Furthermore, the observed activity, potential discoveries, and identification of gaps surrounding a specific problem set will in turn drive current and subsequent collection requirements as depicted in figure 3, with the arrow from "discovery" to "planning and direction." This correlated data discovery will potentially answer questions that were never asked or the analysts were unaware of the answers or how to answer the question in the past. Accordingly, the collection manager and end customer do not necessarily need to know beforehand how the analysts plan to use the data, unlike the traditional targeted collection model. Such a transformation will likely drive predetermined collection decks obsolete, while also enabling the analysts to improve their understanding and build specialized

Distributed Common Ground System–Army Program Manager assesses tactical glasses demonstrated at Enterprise Challenge 13 (U.S. Army/Kristine Smedley)

collection strategies with faster decision cycles and anticipatory analysis.

The first two ABI methodological approaches of georeference to discover and data integration before exploitation with their focus on multi-INT data clustering can enable the discovery of new intelligence in a noisy data environment. Moreover, these new methods can also fundamentally transform the PCPAD and traditional analytic processes to be more responsive to analyst and warfighter needs.

The next pillar to achieving the ABI methodological transformation occurs only when we take a *data (sensor) neutrality* approach. This pillar is predicated on accepting all data sources—that each can potentially be equally viable and that one data source or piece of data is not biased over the other.[17] In this case, an ABI analyst does not favor any particular intelligence discipline (for example, SIGINT) reporting over any other data source (for example, GEOINT synthetic aperture radar [SAR] imagery). Likewise, an ABI analyst must accept a nonspatial or georeferenced data source because it may act as a tip for other sources. For instance, SIGINT or HUMINT data that may have an error of probability that geographically covers a large city and cannot be pinpointed to a specific suburb or facility must be treated as just as viable as a piece of information with exacting coordinates. Also, a fleeting piece of intelligence, like transitory CW preparations and the nonpersistent nature of poisonous gas when employed, must reside at an analyst's fingertips to correlate with the other pattern developing multi-INT data. Additionally, the data must encompass a full range of sources, to include OSINT, especially social media (for example, YouTube).[18] For instance, local Syrian social media reports of the CW attack numbered in the thousands, with hundreds of videos to confirm the attack and highly credible reporting from international humanitarian organizations and hospitals.[19] Of course, an ABI analyst has to understand and account for the confidence, reliability, and potential errors in the data source as well as the interrelationships of what the data from the separate sources are providing and their integrated results.

Much of the collected data prior to an event or abnormal activity, such as the activity observed 3 days prior to the CW attack, would likely appear irrelevant at the time of initial exploitation. However, the observed CW activity can be quickly identified as significant when an ABI analyst applies the *sequence neutrality* approach, the fourth pillar of ABI. Essentially, ABI analysis of the data may happen immediately, or the data may not become relevant until the analyst acquires more data and is able to develop a pattern of activity.[20] As such, previously collected

(continued on page 32)

Five Examples of Big Data Analytics and the Future of ISR

By Jon A. Kimminau

When we talk about U.S. Air Force intelligence, surveillance, and reconnaissance in 2023, we often depict it graphically as beginning with a global array of sensors that produces a variety of data absorbed in a cloud, from which multisource and all-source analysts produce decision advantage for both national and combatant decisionmakers. Big data analytics is at the core of this vision, and its impacts to intelligence analysts and the way they execute their mission will be multifaceted.

How can we describe these impacts? What are some examples or ways to show how big data analytics will work? To answer these questions, we must first understand what is meant by big data analytics and how it can be distinguished from most of our present analysis operations. There are three essential elements to true big data analytics:

- A high volume, velocity, and variety of data with both time and space dimensions from multiple sources are collected and metatagged in an information "cloud."
- Applications that allow analysts to manipulate, visualize, and synthesize the data, leveraging relationships between data elements, must be dynamically developed and accessible.
- Analyst operations on the cloud—their projects, queries, folders, access—must be captured and continuously added to the cloud as additional metatagged data.

Dr. Jon A. Kimminau is a Defense Intelligence Senior Leader and the U.S. Air Force Analysis Mission Technical Advisor.

These three elements are at the heart of big data applications in the commercial and information technology digital space. But more importantly they are at the forefront of future intelligence developments and will greatly impact every activity.

Discovery

Intelligence discovery is the ability to select, manipulate, and correlate data from multiple sources in order to identify information relevant to ongoing operations and requirements. Discovery is about better organizing and using the data that we already know. It is also about finding previously hidden patterns and anomalies—former Secretary Donald Rumsfeld's "unknown unknowns." Imagine in the future that a Pacific Air Forces air operations center analyst is examining air activity in the South China Sea over the past 2 weeks and notes a pattern of flights from select Chinese bases to outposts in the Paracel and Spratly Island groupings. Using an application, the analyst isolates bases of origin and destination and filters the past 4 months of data to visualize the activity. She discovers a pattern that may be a shuttle operation of troops to outposts from which the troops apparently do not return to home base. This activity is then reported by the analyst as a previously unknown buildup of Chinese forces in disputed islands, which may lead to international confrontation. Our ability to discover this kind of activity today is severely restricted by an inability to understand what we have already got. The data are derived from varying sensors, compiled in separate databases, and not accessible and manipulable by any single application. Big data analytics will help us move to a digital "commons," organize our data in uniform manner across all our sources, and then bring new applications for exploring the data to an analyst's workstation.

Assessment

Intelligence assessment is the ability to provide focused examination of data and information about an object or an event, to classify and categorize it, and to assess its reliability and credibility in order to create estimates of capabilities and impacts. Assessment is how intelligence determines what our consumers should be concerned with—and how concerned they should be. Imagine in the future a military strike against a terrorist target in a Central Asian nation, using an unmanned aerial vehicle. Commanders want to know the success of the strike. An analyst, drawing on near-real-time imagery and past information about the site and activity around it, uses an application that detects all changes. In addition, the application provides a visualization of the reactions of both people and objects in the target vicinity. Synthesizing this information rapidly, the analyst can provide near-real-time battle damage assessment to the commander, reporting that the primary physical target was destroyed, that bodies were present, and that vehicles appeared to take some persons away from the target area at speed. Although communications from the high value individual (HVI) ceased at the strike, the vehicle departure with a body is included in the assessment that "the target was physically destroyed; X persons killed and Y possibly injured; therefore, we are confident the HVI

was injured or killed in the action." At another level, the theater commander is apprised in near real time of the results of several simultaneous strikes, providing an assessment of campaign effectiveness. Our ability to execute both kinds of assessment today is hampered by lack of access to multiple sources, varying levels of security controls, a lack of tools to rapidly correlate and visualize the data, and lack of command and control applications to aggregate the reports into a near-real-time campaign battle damage assessment.

Explanation

Intelligence explanation is the ability to examine events and derive knowledge and insights from interrelated data in order to create causal descriptions and propose significance in greater contexts. Explanation is how intelligence provides our consumers narrative stories, relates events to broader situations, and identifies the core of what is going on. Imagine in the future a U.S. European Command analyst is tasked to look at an incident of civil unrest in southeastern Lithuania. After composing and executing a query and defining an area of interest, the system presents not only information on the event in question, but also that a fellow analyst is looking at a similar event in Estonia and that two other events of the past week are under examination by others. Examining the project folders of these analysts, she then follows a thread about Russian troop movements along the borders and an aerial reconnaissance intercept of a North Atlantic Treaty Organization platform by a Russian fighter. Collaborating with these and other analysts, an intelligence estimate is produced that projects a building confrontation of Lithuanian and Estonian separatists with host countries and potential provocation by Russian border elements. This type of assessment is difficult to produce today as data and information sets are often segregated by type of source and regional assignment. In addition, while analysts can collaborate today, it is more often a "pull" system where one asks those who are known to be working a problem, rather than a "push" system where analysts may be automatically alerted to other similar work. Big data analytics expands the avenues for collaboration and multidisciplinary, shared expertise in a global, distributed enterprise.

Anticipation

Intelligence anticipation is the ability to warn and describe future states of the environment based on the manipulation and synthesis of past and present data. Anticipation includes near-term warning and longer term forecasting to alert and prepare decisionmakers to events relevant to their responsibilities. Imagine a Central Air Forces analyst whose responsibility is force protection surveillance of remaining U.S. bases in Afghanistan. Years of experience and lessons learned by the Joint Improvised Explosive Device Organization have been incorporated into system alert templates for a warning application. These templates respond to a variety of intelligence and open-source inputs when activated and focused on designated areas. When a large vehicle being towed on a major road near one base apparently stalls, sufficient indicators in the template create a warning for the analysts of a potential massive car bomb situation. The analyst reports the alert to base leadership and security teams, and protocols are followed to isolate and assess the vehicle. This kind of anticipatory intelligence is possible today only when collection resources are focused to deployed exploitation centers, and analysts there have both attention on the situation and the personal experience to look for appropriate indicators. Big data analytics can incorporate that experience into applications, cast the security net far wider, and recognize potential situations much quicker.

Delivery

Intelligence delivery is the ability to develop, tailor, and present intelligence products and services according to customer requirements and preferences. Delivery is about both intelligence products—from tactical reports to full-blown finished intelligence estimates—and intelligence services, ranging from crew threat briefings to daily intelligence assessments at headquarters to real-time analyst response to requests for information. Imagine a flag officer in a theater combatant command position reading a classified daily briefing on a digital pad. One item deals with a past day event of a U.S. reconnaissance platform being intercepted by an adversary military fighter. The senior leader then taps an icon titled "recent recce [reconnaissance] intercepts" and is provided a list of both local and global intercepts for the past six months. Noting several in his own area of responsibility, the leader also taps an icon titled "recent provocative incidents" and discovers several ship confrontations in international waters and an intelligence estimate and open news media editorial both assessing the increased provocations as being intended to influence an upcoming Secretary of Defense military visit. The ability for a consumer to draw on the context of an intelligence report service for a broader variety of relevant information exists only in a limited fashion today—dependent on extensive, manual preparation of the background data and hyperlinks to it—but a big data infrastructure can automate the foundational background analytics.

Big data analytics offers the potential to revolutionize how analysis supports our warfighters and national decisionmakers with intelligence—the decision advantage in national security. This revolution extends across the spectrum of intelligence analysis activity—from discovery and assessment, to explanation and anticipation, to delivery. JFQ

(continued from page 29)

and archived multi-INT data analyzed in a forensic manner can be as or more important than data obtained near real time.[21] Additionally, an ABI analyst will not be biased toward an archived dataset that was specifically part of the targeted collection deck. In fact, incidentally collected data may be as or more significant than data collected in a targeted fashion. In some cases, data may need to be reexploited and analyzed based on additional information or may be repurposed for a different target within the same collection window.

Establishing the ABI Methodology

The described examples reveal how ABI methodology provides insight earlier in the intelligence process, enabling analysts to spend more time gaining context and analyzing the problem, while machine-to-machine processing interfaces and correlates the georeferenced data automatically. This new paradigm, as reflected in figure 3 (with flipped pyramid), reveals how the DOD intelligence enterprise could shift its model of exploiting approximately 80 percent of the collected data to one focused only on the pertinent 20 percent.[22] By analyzing only the pertinent information and focusing the PED efforts, there will be a net manpower and cost savings to answer the key intelligence questions in an ABI-enabled and discovery focused environment.

The DOD intelligence enterprise must avoid the temptation to focus purely on acquiring the next widget or-specific toolset and focus first on developing the proper big data–enabled analytic environment. Although these developmental ABI toolsets will be invaluable to eventually executing the methodology, the first foundational step for DOD to derive maximum value from its data must be to ensure that the sensor collection-to-analysis timeline is quick enough to detect a pattern. This process must take place in a matter of minutes to be truly actionable by a warfighter, not days (as seen in today's multi-INT analysis paradigm). To accomplish this, the architecture must be able to scale to the level required to retrieve and transmit the vast new and old data sources and store the datasets efficiently for extended periods of time for archival analysis.

Available technologies such as the Cloud and High Performance Computing with advanced algorithms have matured rapidly and may provide the proper solution space to handle the data storage dilemma and processing of complex datasets that enable ABI. However, the Cloud and High Performance Computing do not completely resolve the requisite architecture and bandwidth requirements to transmit and retrieve large disparate datasets from the sensor to the analyst in a timely fashion.

The time is right to move toward an integrated DOD and national intelligence enterprise architecture "with budget realities, current state of technologies and a sense of urgency in the IC leadership all combining to create an optimal climate for positive change," according to the IC Chief Information Officers in an IC Information Technology Enterprise (ITE) white paper.[23] In 2012, the Director of National Intelligence moved to transform a historically agency-centric IT approach to a new model of common architecture—labeled IC ITE, which will provide the IT shared services model for the national IC. The five leading national intelligence agencies—Central Intelligence Agency, National Security Agency, National Geospatial-Intelligence Agency, Defense Intelligence Agency, and National Reconnaissance Office—have combined efforts to move the community to a "single, secure, coherent, mutually operated and integrated IC IT Enterprise."[24] With over 70 percent of the IC under DOD, the IC and DOD have ideally paired to share a common vision and have a similar timeline and path ahead to ensure a broader intelligence enterprise approach. The DOD and IC share the same vision but are working on parallel solutions that are not necessarily creating a completely integrated intelligence enterprise with analytical transparency—allowing a seamless collaborative environment.[25]

The Defense Information Systems Agency (DISA) has been charged with the herculean task of consolidating and integrating multiple DOD networks into one common, shared network known as the Joint Information Environment (JIE). Ostensibly, the JIE currently faces the challenge of interacting and competing DOD program offices and being funded only by participants who desire increased IT efficiencies. Furthermore, the IC ITE task force recently stated that the JIE "is neither an enterprise (requiring common mission and leadership) nor an architecture (requiring tight management of implementation)."[26] In fact, Admiral David Simpson, DISA Vice Director, pointed out that the JIE "is not a program of record or a joint program office."[27] This troubling state of affairs suggests that DOD should reexamine the JIE and the end-goal of creating a common, integrated network when it does not include complete DOD buy-in, and more important, is not in sync with the IC ITE construct. This two-pronged approach with both JIE and IC ITE will drive many DOD intelligence organizations to pick between the two or, even worse, to have to develop a hybrid system that interacts with both. In fact, the Air Force ISR 2023 strategy contends that to handle the challenges of data overflow and to transform to an ABI methodology, the Air Force ISR enterprise must be a "full partner of the IC-ITE and JIE."[28] This approach portends an enterprise with uncommon IT services, disparate architectures, and an untenable budget during a more constrained economic environment.

Conclusion

Using the four-pillared approach, ABI will provide solutions to assembling an answer by fitting small bits of linked yet disparate information from brief ISR windows into a complete picture. This will enable analysts to pull meaningful images from a sea of pictures, enabling discovery and greater context across the fabric of data for subsequent analysis. The success of ABI relies on the inte-

gration and correlation of truly large amounts of multi-INT data, as well as the tools to handle and appreciate what the ABI methodology is revealing. Many analysts coming out of operations in Iraq and Afghanistan presuppose that ABI is only enabled by persistently collected data, like ubiquitous full-motion video, on activity and transactions over a broad area. However, ABI truly harnesses big data by using a variety of integrated sources regardless of sensor platform. Even in contested battlespaces such as the hypothetical CW example, ABI does not necessarily depend on 24/7 sensor coverage—it builds on a variety of multi-INT data that can be integrated to fill holes in sparse single-source datasets.

The DOD intelligence enterprise must look over the horizon to an ABI analytic environment where such ISR sources as streaming FMV, MTI, OPIR, SIGINT, MASINT, SAR, spectral, and thermal imagery are integrated at the post-processed and georeferenced entry point and compared with archived collected data in an automated fashion. By harnessing a new IT environment enabled by ABI methodologies, analysts will be able to rely on readily available high-speed machine-to-machine processing and big data to make ABI possible on a large scale. These intuitive concepts will require significant effort and a unified IC strategy to overcome the technical and cultural challenges of developing such an information-sharing environment and paradigm-shifting approach to the traditional intelligence process.

During the Cold War, the IC had a laser focus on the adversary and became adept at distinguishing and even predicting Soviet strategic bomber activity and surface-to-air missile TTPs because they possessed discernable signatures, and those signatures were embedded in doctrine. Today, the IC faces more dynamic and multifaceted adversaries that possess fleeting signatures and minimally supporting doctrine. The DOD intelligence enterprise must collectively invest in the ABI tools, develop analyst tradecraft, and embrace a transformed intelligence process to repossess this level of understanding. Only then will we be able to address the near peer countries and asymmetric threats, exhibiting weak and nonpersistent signatures for tactical and strategic production needs. **JFQ**

Notes

[1] Robert P. Otto, *Air Force ISR 2023: Delivering Decision Advantage* (Washington, DC: Headquarters Department of the U.S. Air Force, 2013).

[2] Lydia Ines Rivera, Debbie Salierno, and Allen Siwap, "Multi-Intelligence Distribution Architecture," Capstone Team Project, University of California, San Diego, 2013.

[3] Michael W. Isherwood, *Layering ISR Forces*, Mitchell Paper 8, (Arlington, VA: Mitchell Institute Press, December 2011).

[4] John K. Langley, "Occupational Burnout and Retention of Air Force Distributed Common Ground System (DCGS) Intelligence Personnel," RGSD-306 (Ph.D. diss., Pardee RAND Graduate School, 2012).

[5] Michael Farber et al., *Massive Data Analytics and the Cloud: A Revolution in Intelligence Analysis* (McLean, VA: Booz Allen Hamilton, 2011).

[6] Letitia A. Long, "Activity Based Intelligence: Understanding the Unknown," *The Intelligencer* 20, no. 2 (Fall/Winter 2013), 7–15.

[7] David Gauthier, "Activity-Based Intelligence Definition for the Intelligence Community," National Geospatial-Intelligence Agency, 2013.

[8] Jon Kimminau, author interview, October 18, 2013.

[9] Gauthier.

[10] "Government Assessment of the Syrian Government's Use of Chemical Weapons on August 21, 2013," The White House, August 30, 2013.

[11] Shane Harris et al., "U.S. Had Intel on Chemical Strike Before It Was Launched," *Foreign Policy*, August 30, 2013.

[12] Gauthier.

[13] Mark Phillips, "A Brief Overview of Activity Based Intelligence and Human Domain Analytics," *Trajectory*, 2012.

[14] Gauthier.

[15] Ibid.

[16] Joint Publication 2-01, *Joint and National Intelligence Support to Military Operations* (Washington, DC: The Joint Staff, 2012).

[17] Gauthier.

[18] Kristin Quinn, "A Better Toolbox: Analytic Methodology Has Evolved Significantly Since the Cold War," *Trajectory* (Winter 2012), 1–8.

[19] "Government Assessment."

[20] Quinn.

[21] Gauthier.

[22] Robert Jimenez, presentation, Big Data for Intelligence Symposium, Defense Strategies Institute, November 2013.

[23] Accenture, "Driving High Performance in Government: Maximizing the Value of Public-Sector Shared Services," The Government Executive Series, January 2005; Terry Roberts et al., White Paper, "Intelligence Community Information Technology Enterprise: Doing in Common What Is Commonly Done," Intelligence and National Security Alliance, February 2013.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] Amber Corrin, "JIE's Murky Progress Raising Questions," *FCW* [Federal Computer Week], August 27, 2013.

[28] Otto.