Lieutenant General Vincent Stewart, USMC, delivers inaugural address as director of Defense Intelligence Agency and commander of Joint Functional Component Command for Intelligence, Surveillance, and Reconnaissance, January 23, 2015 (Defense Intelligence Agency)

Transforming Defense Analysis

By Catherine Johnston, Elmo C. Wright, Jr., Jessica Bice, Jennifer Almendarez, and Linwood Creekmore

The Defense Intelligence Enterprise is on the precipice of tremendous change. The global environment is experiencing a mind-numbing quantity and diversity of challenging crises. Perhaps not since the end of World War II have so many pockets of instability and change confronted the Intelligence Community (IC). These traditional security crises are compounded by global demographic, economic, and climate challenges that need to be viewed through the prisms of nontraditional disciplines.

Against the backdrop of this complex operational environment, the volume, velocity, and variety of data continue to grow at a dramatic pace.[1] The early 21st century has seen groundbreaking disruptive technologies adopted on a global scale, and the pace of technology innovation and further disruptive developments looks to increase exponentially. Drivers of technology innovation are no longer simply government-funded initiatives; commercial and private industries are also involved. Individuals are increasingly empowered with a low barrier of entry for truly sophisticated technological fields. The IC must take advantage of this seemingly boundless information age by leveraging large volumes of data, using

Catherine Johnston is Director for Analysis at the Defense Intelligence Agency (DIA). Elmo C. Wright, Jr., is the Senior Expert for Analytic Modernization and Innovation at DIA. Jessica Bice is an Intelligence Officer in the Defense Counter Terrorism Center at DIA. Jennifer Almendarez is a Strategic Communications Officer at DIA. Linwood Creekmore is an Analyst at DIA.

innovative technology, and employing common analytic strategies and tradecraft to provide the United States and its allies with critical information when and where it is needed.

The Defense Intelligence Agency (DIA) recognizes that the collective response of these defense all-source enterprises to such challenges will be significantly limited by the stark realities of fiscal austerity. The intelligence budget is unsustainable given fiscal pressures, and yet it is inadequate considering the scope and scale of current and future operational requirements. The solution will not be in lobbying for additional funds—mandated reductions and decreased budget authorizations must be adhered to—but rather in effectively transforming our tradecraft and technology. We are addressing the threat environment by aligning our priorities with the 2014 National Intelligence Strategy objectives: innovating the way we share data while safeguarding it, managing the defense intelligence analytic enterprise, investing in our people, and working with our partners.[2] In this article, we examine in turn how we are doing in each of these four areas. The article then concludes with what the future of defense all-source analysis might look like.

Innovating Information-Sharing While Safeguarding Data

The defense intelligence ecosystem has evolved rapidly over the past 10 years, but our analytic methodologies have only incrementally adapted to the changing environment. As of 2012, more than 90 percent of the stored data in the world had been created in the previous 2 years.[3] Historically, information in the IC was disseminated through single intelligence discipline stovepipes according to the specific sensor that detected it. This method of receiving data forced the all-source analyst to hunt for and gather information in these stovepipes—basically finding all of the disparate pieces of information and acting as the manual fusion engine for single-source reporting. Given the manual method of collecting information, we estimate that at least 70 to 80 percent of an all-source analyst's work hours is spent searching and compiling information, and less than 20 percent is actually spent performing higher order analytics of the assembled data.[4]

The crux of this inefficiency is the onset of large electronic data sets that have created challenges for analysts in how they retrieve, mine, and amalgamate information to glean key insights. As automated data expand, analysts are overwhelmed, with no reasonable chance to find all the relevant information, much less analyze it. Instead, analysts spot-check roughly 1,400 data sources for information they believe will be most relevant.[5] This introduces hidden biases, as analysts are more likely to seek data sources that reinforce their preconceived opinions. Unfortunately, data can become operationally useful only if we can make sense of it at the right time and in the right context. The intelligence analytic enterprise must find a way to ensure analysts can access data from areas, tools, and platforms not previously discoverable. This challenge is the driving force behind DIA's analytic modernization initiative.

Working in conjunction with the Director of National Intelligence's information technology strategy, the IC Information Technology Enterprise (IC ITE, or "I sight"), and the Mission User Group, DIA is facilitating this fundamental shift in the analytic environment. The IC ITE architecture will enable the Intelligence Community to become more transparent, efficient, and effective, moving us from an individual, agency-centric model to an enterprise model that shares resources and data. The common cloud-based data architecture will reconcile single-source, multi-source, and all-source collection and analysis in near real time. This new IT architecture provides a tremendous opportunity to reimagine our intelligence process in ways that eliminate dissemination stovepipes, increase multi-intelligence data-sharing, and integrate knowledge at the data layer, thus eliminating, or at least reducing, the existing linear and labor-intensive tasking, collecting, processing, exploiting, and disseminating process. IC ITE will significantly enable and make easier a number of cross-agency analytic modernization efforts, such as object-based production (OBP).

Object-based production is a concept being implemented as a whole-of-community initiative that fundamentally changes the way the IC organizes information and intelligence. Reduced to its simplest terms, OBP creates a conceptual "object" for people, places, and things and then uses that object as a "bucket" to store all information and intelligence produced about those people, places, and things. The object becomes the single point of convergence for all information and intelligence produced about a topic of interest to intelligence professionals. By extension, the objects also become the launching point to discover information and intelligence. Hence, OBP is not a tool or a technology, but a deliberate way of doing business.

While simple, OBP constitutes a revolutionary change in how the IC and the Department of Defense (DOD) organize information, particularly as it relates to discovery and analysis of information and intelligence. Historically, the IC and DOD organized and disseminated information and intelligence based on the organization that produced it. So retrieving *all* available information about a person, place, or thing was primarily performed by going to the individual repository of each data producer and/or understanding the sometimes unique naming conventions used by the different data producers to retrieve that organization's information or intelligence about the same person, place, or thing. Consequently, analysts could conceivably omit or miss important information or erroneously assume gaps existed.

OBP aims to remedy this problem and increase information integration across the IC and DOD by creating a common landing zone for data that cross organizational and functional boundaries. Furthermore, this business model introduces analytic efficiency; it reduces the amount of time analysts spend organizing, structuring, and discovering information and intelligence across the enterprise. By extension, OBP can afford

analysts more time for higher orders of analysis while reducing how long it takes to understand how new data relate to existing knowledge. A central premise of OBP is that when information is organized, its usefulness increases.

A concrete example best illustrates the organizing principle of OBP and how it would apply to the IC and DOD. Consider a professional baseball team and how OBP would create objects and organize information for all known people, places, and things associated with the team. At a minimum, "person" objects would be created for each individual directly associated with the team, including coaches, players, the general manager, executives, and so forth. As an example of person-object data, these objects would include characteristics such as a picture, height, weight, sex, position played, college attended, and so forth. The purpose is to create, whenever possible, objects distinguishable from other objects. This list of person-objects can be enduring over time and include current and/or past people objects or family or previous team relationships.

In a similar fashion, objects could be created for the physical locations associated with the team, including the stadium, training facility, parking lots, and players' homes. The same could be done for "thing" objects associated with the team, such as baseballs, bats, uniforms, training equipment, team cars/buses/planes, and so forth.

With the baseball team's objects established, producers could report information to the objects (for example, games, statistics, news for players, or stadium upgrades), which would serve as a centralized location to learn about activity or information related to the team. Also, relationships could be established between the objects to create groupings of objects that represent issues or topics. For example, a grouping of people-objects could be created to stand for the infield or outfield, coaching staff, or team executives. Tangential topics/issues such as "professional baseball players involved in charity" could be established as well. Events or activities (such as games) and the objects associated with them could also be described in this object-centric data construct. Moreover, the concept could expand to cover all teams in a professional baseball league or other professional sports or abstract concepts that include people, places, or things.

Similar to the example above, the IC and DOD will create objects for the people, places, things, and concepts that are the focus of intelligence and military operations. Topics could include South China Sea territorial disputes, transnational criminal organizations, Afghan elections, and illicit trade. Much like the sports example, IC and DOD issues have associated people, places, and concepts that could be objects for knowledge management.

OBP is dependent on implementation, evolution, and maturation of policies and technologies to set the conditions for IC and DOD transition to OBP as a core production process. OBP services—as they relate to object management, data storage and availability, access control, and security—will largely depend on the infrastructure, policies, and capabilities that come with IC ITE.

OBP services will be delivered as a back-end cloud-based platform service within IC ITE and take full advantage of enterprise security capabilities related to access control and auditing.[6] IC ITE will establish and recognize the electronic identity for all users across the IC and DOD enterprises, with a computer-recognizable understanding of the types of data that each user is allowed to access, regardless of agency affiliation.[7]

This IC ITE capability perfectly complements OBP's data-conditioning standards to "atomize" data. Within the OBP framework, as data are objectified, individual data fragments (such as individual facts about the object) will be tagged with a classification. This is effectively called *atomization* of data.[8] Combining OBP's data atomization and IC ITE's enterprise capability to recognize user access privileges, object views will be assembled dynamically based on the role, authorities, and access of the individual user at machine speeds on enterprise IC and DOD data, regardless of agency affiliation.[9] This is important not only for data access control measures but also for data-auditing purposes. Enterprise managers will have a retrievable history of the types of data each user accessed, potentially at the specificity of knowing which individual object facts were retrieved.

The path forward faces significant challenges. Existing stovepiped processes are well entrenched in DOD. Even in its early stages, IC ITE will change both analytic behavior and intelligence processes, though current pilot programs are not fully operational because the architecture is still stabilizing. Until we have a stable architecture, we must maintain the legacy system, data, and associated processes. IC ITE–enabled analytic integration and exposure to sources of data at the point of system ingestion will provide a much richer knowledge pool; however, this integration will require a concerted change-management program to standardize changes across the Defense Intelligence Enterprise and the IC.

Analytic efficiency, increased productivity, and a stronger, more robust intelligence enterprise are the promises of analytic modernization. These big data–enabled gains across the IC are particularly critical in a time of fiscal austerity and an increasingly complex operational environment. Austerity and complexity will compel the community to function as a cohesive, integrated, and responsive unit. The pilot programs are already driving cultural and behavioral changes for both collectors and analysts. Continued community innovation in data-handling methods will increase collection efficiency and analytical accuracy. Ultimately, these efficiencies will translate into heightened responsiveness and accuracy when meeting the demands of warfighters, policymakers, and national leaders.

In the future, an analyst will begin the day at both the operational and strategic levels by reviewing automated aggregated data and deciphering anomalies to instantaneously begin interacting with key strategic, operational, and tactical colleagues. Collectors and analysts working together in a networked, nonstovepiped environment will leverage collaboration to focus collection and

analytic assessments when informing decisionmakers. Though these pilot programs are in their nascent stages, DIA is committing time and resources to ensure successful, full-operating capability. These pilot programs are the basic building blocks that will enable the true transformation of defense all-source analysis.

Managing the Defense Intelligence Enterprise

Leveraging the Defense Intelligence Analysis Program. A centralized management structure of the Defense Intelligence Enterprise is necessary to drive down duplication and create efficiencies across the enterprise to meet the mission in an era of declining resources and growing requirements. The Defense Intelligence Analytic Program (DIAP) Enterprise includes DIA, nine combatant commands, five Service intelligence centers, two subunified commands, and the Commonwealth partners. Functionally managed by DIA's Directorate for Analysis, DIAP ensures resources are properly aligning to each enterprise member's core mission areas as defined by the National Intelligence Priorities Framework.

Prior to 9/11, the DOD Intelligence Production Program (DODIPP) was the managing entity of analytic production components in the department. After 9/11, the establishment of DIAP dismantled the unpopular DODIPP in favor of a decentralized program that essentially allowed each member to perform the entire breadth of capabilities for its respective organizations, which in turn created enterprise-wide duplications and redundancies. DIAP shifted the focus from quantity of production to level of effort by measuring outcomes rather than counting products. In this case, "outcomes" refers to things that took place as a result of analytic effort, such as operations or special activities.

After DOD funding decreased in 2014 and 2015, DIAP was the only vehicle through which the enterprise could implement changes to defense intelligence processes adjusted to diminished resources. Today, DIAP manages risk mitigation and requirements prioritization. The new era of defense intelligence analysis demands collaboration among all analytic partners. Reduced funding countered by increasing requirements necessitates unified effort and much tighter integration among enterprise members. Primary responsibility resides where primary capability resides, and this critical synchronization of enterprise capabilities not only creates trust among members, but it also enables necessary transparency under the new paradigm of shared responsibility.

Director of National Intelligence James Clapper gives testimony before Senate Intelligence Hearing, January 30, 2012 (Kit Fox/Medill/Flickr)

Technology Solutions to Provide Transparency. DIA is investing in the transparency needed to maximize the efforts of every analyst with a suite of initiatives and tools. The Source is a consolidated production portal that will function as an aggregator of all finished defense intelligence, regardless of organization, on one site. It will improve and increase discoverability for customers, reduce the likelihood of duplicative production, and bolster the expectation that intelligence analysis relies on the existing body of knowledge. The next generation of The Source and the underlying technologies, such as Defense Intelligence Online, will add tools related to production management, tasking, and individual profiles.

One capability enables analysts and customers to see trending analytic subjects based on usage from across the enterprise. This capability makes use of an existing technology that tracks intelligence use and aims to correlate production and usage data for better security, business analytics, and customer service. In addition, production data are mined to provide a "Find the Expert" capability that ensures customers are able to contact an expert for follow-on questions or for future collaboration across the enterprise on any given topic searched. By investing in better tools to capture analytic levels of effort (business analytics), we enable

greater insight that allows every member of the defense intelligence all-source analytic community to understand where the enterprise must focus its efforts. Ensuring that these technologies and data schemas are common across the enterprise also ensures a transparent baseline of information to make more informed decisions.

Investing in Our People

Training and Career Management for Common Understanding. In the longer term, training and tradecraft that foster confidence and trust in products across the enterprise will need to be addressed. Currently, even if analysts find the right expertise or product, they must be confident that their own analytic rigor is mirrored in the products authored by outside organizations. Even with all of the tools and communication vehicles available to analysts, an uncoordinated product that is duplicative is easier than trying to leverage outside expertise for a collaborative, more holistic product.

To build the levels of professional trust and skills needed for this degree of sophisticated collaboration, DIA is making strategic investments in training, education, and professional development. We will establish and measure critical analytic skills for the Defense Intelligence Enterprise through the analyst professional certification program. The program will assess analyst knowledge and performance of critical skills and emphasize continuous analytic proficiency through lifelong learning. These shared skill standards will ensure analysts in the Defense Intelligence Enterprise are synchronized in their use of analytic tradecraft.

Improving and adhering to standards ensure that all-source defense intelligence analysts are equipped with the best tradecraft and skills to perform at peak levels. We have graduated two foundational Professional Analyst Career Education classes for new DIA analysts who received extensive formal training in their first 6 months. We also have developed a curriculum, which was rolled out in October 2014, geared for midlevel analysts and has graduated six classes. We are also refreshing our senior ranks with a 3-day executive version—the third class was just completed in September.

This robust training will give analysts the skills for foundational and advanced analytic tradecraft, and incorporate the latest intelligence and academic methods related to military capabilities, network analysis, sociocultural analysis, analytic design, and alternative futures. Most importantly, this professional development will ensure a superior level of tradecraft. Investing in common training standards will instill a culture of trust by creating analytic cohesion and transparency. This strategy is a cost-effective way for the greater Defense Intelligence Enterprise to minimize duplication and bolster existing networks to create analytic reserve strength. Moreover, DIA understands the need for hiring individuals with nontraditional skills who can operate in an environment where tools and methodologies must change as quickly as data evolve.

That said, the major challenge over the next decade is to develop intelligence officers who better understand the IC apparatus. Analysts must have a broader range of experiences outside traditional intelligence analysis, in both strategic and operational environments. We need analysts who understand nontraditional sources, work comfortably inside collection platforms, fully comprehend the strategic and operational needs of the broad set of defense customers, and can drive focused collection to address key intelligence gaps by using quantitative methodologies and innovative tools. In the fiscally austere future, actively managing intelligence officers will be critical to ensure a collaborative, trusting, and efficient enterprise.

Working with Our Partners

In an increasingly complex world with a wide range of collection targets, we must take advantage of not only our own intelligence assets but those of our foreign partners as well. DIA has always recognized the enormous value of coalition partners and the added value they bring to collection and analysis. Their collaborative participation has provided an important outside perspective that has informed our own in production of strategic defense intelligence in both joint and combined environments. We must understand the culture of our allies' intelligence services and that their intelligence collection employs different methods, under different assumptions, and with different analytical lenses. Understanding these differences up front facilitates seamless exchanges during times of crisis, when relationships are put to the test and are the most valuable.

The United States and its allies possess comparative advantages in different regional and functional areas. This potential allied strength should be leveraged through delineating analytic areas on which we can be interdependent. For example, one of our allies may have a comparative advantage in a part of the world where the United States is less engaged. By relying on that ally's expertise to cover that part of the "intelligence perimeter," we can realign our focus on problems where our strengths lie. Such mission-sharing is a smart investment for the enterprise and the broader Intelligence Community.

This interdependence requires a high level of trust and mutual commitment between the United States and its intelligence partners, as well as the acceptance of some risk in those areas and the loss of the expert knowledge that comes with the day-to-day focus on them. Yet in a time of fiscal austerity, deepening partnerships will expand our capacity to understand the operational environment in mission areas with limited focus. This is a fundamental reason that DIA established its Five Eyes Center, with Commonwealth allies working alongside U.S. analysts to develop more efficient and effective intelligence-sharing practices while breaking down cultural-sharing barriers.

Impediments to better integration with our allies are a combination of a traditional reluctance to share sensitive information and policy and information technology issues. These barriers must be overcome. With analytic modernization efforts based in technology improvements, information-sharing becomes

easier for even the most junior analyst. As that tagging of data is completed at the "atomic" level, making the information releasable without revealing sourcing becomes automatic. When analysts can see the shared knowledge, collaboration with allied partners becomes easier.

In the mid-term, DIA has placed resources and people to reexamine our security policies in light of the current information environment. When information is shared in near real time and highly dynamic situations render analysis perishable, we cannot afford a lengthy release process. We must put in place the proper authorities and develop agreements or understandings with allies to mitigate becoming mired in process. Over time, an ad hoc patchwork of agreements will do little to address the holistic concerns dealing with releasability. The IC challenge is to ensure the range of policy and authorities related to the complex question of releasability deals with the current operational environment and technology.

Our allies and partners have been an integral part of how we overcome the complex operating environment that requires both policy and technical solutions to optimize our collaboration. Synchronization of these efforts holds great promise for focusing and integrating the capabilities of DIA with those of our allies and partners.

The Future Look of Defense All-Source Analysis

The challenges that defense intelligence faces are complex and will require innovative solutions if we are to maintain a strategic advantage. Fortunately, more than a decade of integrated operations in the field has provided a blueprint. Joint operations have already proved that the hardest problems are solved not by a single intelligence discipline or single agency. Breakthroughs derive from technological advances that naturally enhance cross-intelligence discipline collaboration and elimination of organizational and cultural barriers. Yet the field is not the hallways of Washington, and the operational boundaries between brigades are not the interagency community. What worked in a forward area cannot always be generalized to another venue, and we do a disservice if we try to directly translate lessons that worked in an interagency task force in Afghanistan to a large and complex organization such as DIA without adapting such lessons to the scale of the organization and the unique processes inherent therein.

Afghan National Army soldiers wait for updates during runoff elections at Forward Operating Base Gamberi, Laghman Province, Afghanistan, June 14, 2014 (U.S. Army/Dixie Rae Liwanag)

The operational interaction with intelligence will look different in the future. Historically, operators have been given a lengthy analytic paper or a large intelligence annex describing enemy composition, disposition, and most likely courses of action. In the future, using analytic models of enemy doctrinal templates, the IC will create a dynamic environment that will enable the warfighter and policymaker to interact with enemy weapons systems, command and control apparatus, and doctrine in a more dynamic, iterative environment.

A current example of this modeling and simulation (M&S) technique has been developed at DIA's Missile and Space Intelligence Center (MSIC). MSIC analysts, in close cooperation with their National Air and Space Intelligence Center (NASIC), National Ground Intelligence Center (NGIC), and Office of Naval Intelligence/Farragut Technical Analysis Center (ONI/FTAC) counterparts, are providing combatant commands with projected threat capabilities to counter U.S. contingency operation plans. These threat performance assessments, requested specifically by the planning elements at the major commands, have led to significant modifications to existing contingency plans, including target allocations; munitions selection platform routing; weapons tactics; targeting rules of engagement; and intelligence, surveillance, and reconnaissance placement. These innovative techniques, refined through years of iterative process improvement, are now adopted for use in the U.S. research, development, and acquisition communities.

Building on these M&S-based analyses for the combatant commands, MSIC is leading development of the next generation of integrated analysis capability. The Integrated Threat Analysis and Simulation Environment (ITASE) provides DOD with a modeling and simulation capability to predict the holistic performance and effectiveness of foreign and U.S. weapons systems and plans. ITASE, which is jointly developed by DIA/MSIC and NASIC, NGIC, and ONI/FTAC, establishes a standard solution for integrated weapons system modeling, simulation, and analysis across

Japanese nationalist far-right group Ganbare Nippon stages Senkaku Islands protest, January 23, 2013 (Wikimedia Commons)

intelligence production centers. The environment brings together disparate weapons systems models from different IC organizations to evaluate complex scenarios, including examinations of antiaccess/area-denial and contested and degraded environments. This type of analysis is the future and is integral to how customers interact with the avalanche of intelligence data.

Leaders of large intelligence organizations must take what action they can to overcome obstacles that organizational history presents them. This future of a modernized analytic environment will succeed only when leaders foster the breakdown of single-source stovepipes, invest in the modernization of analysis, drive efficiencies across the enterprise, invest in people, and partner with our allies. The real art of such leadership is to identify the key elements that will change the organizational culture and to work to operationalize those elements.

Defense intelligence must become better organized, and the synchronization effort through the leadership of DIA can increase cooperation throughout the defense intelligence all-source analytic community, increasing the cogency of analytic effort and the effectiveness of collection. The challenges of big data that analysts face will be mitigated by how we develop our personnel and the tools and concepts we provide that optimize their abilities.

Ultimately, DIA must support the warfighter across the spectrum of military operations; that is the benchmark by which all of our actions must be measured. In the 21st century, warfighting effectiveness includes a great deal more than active combat; it includes the full range of military options open to our national leadership, from security force assistance to nuclear war. The Defense Intelligence Agency and the defense intelligence all-source analytic enterprise must position themselves for success now and in the future, creating a collaborative intelligence environment with allies, partners, and the Intelligence Community. **JFQ**

Notes

[1] General Keith Alexander, USA (Ret.), "Closing Remarks at Accumulo Summit, June 2014," June 12, 2014, available at <http://accumulosummit.com/archives/2014/program/talks/>.

[2] *The National Intelligence Strategy of the United States 2014* (Washington, DC: Office of the Director of National Intelligence, 2014).

[3] Rosemary Heiss, "GEOINT IT Changing to Better Support Analysts, Integrated Intelligence," *Pathfinder* 10, no. 1 (September–October 2012), 6–7, available at <www1.nga.mil/MediaRoom/Press%20Kit/Documents/Pathfinder%20Magazines/2012/2012_sept-oct.pdf>.

[4] Steve Lohr, "For Big-Data Scientists, 'Janitor Work' Is Key Hurdle to Insights," *New York Times*, August 17, 2014.

[5] Heiss.

[6] Chief Information Officer (CIO), Office of the Director of National Intelligence (ODNI), "Enterprise Audit," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/enterprise-audit>.

[7] CIO, ODNI, "IdAM: Full Service Directory," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/idam-full-service-directory>.

[8] CIO, ODNI, "REST Service Encoding Specifications for Security Markings," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/rr-security-markings>.

[9] CIO, ODNI, "XML Data Encoding Specification for Need-To-Know Metadata," *DNI.gov*, available at <www.dni.gov/index.php/about/organization/chief-information-officer/need-to-know-metadata>; CIO, ODNI, "REST Service Encoding Specifications for Security Markings."