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.

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

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

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