The Big Data Imperative

Air Force Intelligence for the Information Age

Col Shane P. Hamilton, USAF

Lt Col Michael P. Kreuzer, USAF, PhD*

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

Big data is the subject of much discussion in the media and in the government today. It has been described as an "easy button," when combined with artificial intelligence, to reduce the human role of analysis. Some view this as a potential threat to the democratic order, and by others it is viewed as a lot of hype with few earth-shattering results to show.[1] What is big data, and why is it vital to the future of the intelligence community (IC) and combined military operations?

In this article, the authors argue that the information revolution has radically changed intelligence by dramatically increasing the number and variety of intelligence collectors. Thereby the collectors create a global network of analysts and

*The authors would like to thank those who provided key insights and reviews for this article, including Kenneth Bray, Dr. Jon Kimminau, Lt Col Shawn Smagh, and Maj Shaun Lee.

machines that facilitate the rapid sharing of data and information. This network also increases the appetite of operators for faster and more operationally relevant assessments about threats and targeting opportunities. Further, it has reshaped the threat environment by creating new centers of power and collection in the cyber domain—where adversaries can recruit members, plan strikes, and exploit both ordered and inspired attacks through online collectives. Our current manpower and resource-constrained environment—combined with these factors—necessitates new strategies for planning and executing intelligence, surveillance, and reconnaissance (ISR) operations, and investment in organizing, training, and equipping analyst Airmen with the tools to succeed in the modern information environment. Big data conceptually sits at the core of this environment and will drive our understanding of how we collect, structure, and analyze data, information, and intelligence in the future.

Cutting through the Hype—What is Big Data?

As the name implies, *big data* is ultimately about the gathering, storing, and processing of large volumes of data and information. Intelligence analysts will quickly point out that there is nothing new about gathering and storing large volumes of information, as it has been a central purpose of intelligence entities for centuries. Nonmilitary analysts regularly sort through large volumes of data to make quantitative assessments of complex problem sets based on tens of thousands of case observations across multiple variables. So, what makes big data new and different? The phrase first appeared in the early 2000s, when industry analyst Doug Laney defined big data as distinct from previous models by three main factors dubbed the "three Vs:"[2]

- **Volume**—The information age enables both the acquisition and storing of data and information that can be preserved and regularly accessed and analyzed on scales not seen before. Most previous databases for analysis could be contained in a single database (such as a Microsoft Excel database) with lines ranging from tens to tens of thousands of lines. Big data enables the collection of millions to billions of data points.
- **Velocity**—The volume of data and information is acquired at an unprecedented speed and must be dealt with promptly. Twitter, for instance, received 500 million updates (tweets) per day in 2013;[3] each tweet constituting a single data point of information.
- **Variety**—Data and information come in numerous formats from diverse sources. In the past, the analyst or entity requiring the information could shape what was collected and how it was stored, but the combination of volume and velocity today necessitates building systems to manage and incorporate data in the form in which it is acquired; from an image to a Twitter or Facebook entry to a transcript of a conversation or speech.

As awareness of big data has grown, many scholars today have added to these three Vs with other dimensions such as variability and complexity. In the USAF, among other institutions, we add a fourth "V" to this list:

- **Veracity**: The volume, velocity, and variety of data accessible via big data include a significant amount of noise and irrelevant data to the problem set. This creates potential abnormalities in data analysis and opens the door for analytic bias in the selection of what data is important and how to analyze it. Big-data strategies must include processes to keep data "clean" and an analytic awareness of the big data working hazards.

After big data emerged, a new phrase—*big-data analytics* —came into vogue.[4] These terms are often thrown about interchangeably but represent two distinct sides of the same coin. Big data represents a process for rapidly compiling, storing, and accessing large amounts of data and information from numerous sources and with varying structures. Big-data analytics represents the tools, tradecraft, and processes that can transform big data into insights—from intelligence preparation of the operating environment to threat warning to predictive battlespace awareness to targeting. These insights in turn shape decisions across the range of military and diplomatic operations, from strategic deterrence operations to near- real-time (NRT) tactical engagements.

Debates about big data's potential versus hype stem largely from misunderstanding both big data and big-data analytics.[5] Big data's cheerleaders have historically made four exciting claims about big data that are at best optimistic oversimplifications: (1) data analysis produces uncannily accurate results; (2) sampling is unnecessary because big data allows us to capture all possible data points; (3) high levels of correlation in big data makes qualitative debates about causation passé; and (4) statistical models are similarly irrelevant because "the data speaks for itself."[6] In truth, big data doesn't eliminate traditional challenges in data collection and data analysis; it does radically reshape where and how the snags occur. The main challenge stems from the final claim: data never speaks for itself. The manner in which data is gathered, organized, and processed shapes the message that the data sends to the user. Complex algorithms perform many of these functions to enable big data analytics, but those algorithms, even facilitated by machine learning, must be programmed by humans and tailored to answering prespecified questions.[7] This means big data is still subject to biases in collection, display, and analysis of which analysts must be acutely aware. Big data enables access to exponentially increasing data points to facilitate faster analysis from more data points, but bad big-data analysis begets bad analysis.

How Big Data Reshapes Intelligence

Of the four Vs of big data, analysts have until recently had to contend mainly with the first and third "V," but on a smaller and more manageable scale. The pace of collection, the relative consistency of threats posed by state actors, and the stovepiping of analysis and production along intelligence discipline production lines (the INTs—signals intelligence [SIGINT], geospatial intelligence [GEOINT], imagery intelligence [IMINT], human intelligence [HUMINT], open-source intelligence [OSINT], and measurement and signals intelligence [MASINT]),[8] enabled the division of effort into separate data problems that could be analyzed in parts by specialists, with all source intelligence answers produced by combining component parts.

The information revolution's impact on USAF intelligence's core competencies (collection, analysis, targeting, and integration) focused first on collection and second on both threat and targeting analysis (see fig. 1). There has been a dramatic increase of collectors and sensors available, with globally integrated ISR enabling NRT exploitation. Concurrently, operational demands shifted analysis for both threat and targeting analysis toward NRT to get inside the adversary's OODA loop.[9] In an era of constrained resources with few signs of significantly increased manpower in the near future, changing intelligence production to meet today's operational demands is unlikely to come from further revolutionizing collections or analysis. Today, even within the INTs, the volume, velocity, and variety of data and information collection has grown to a point where analysts can no longer sift through everything collected sufficiently to even store—much less analyze—all of it without the aid of computer programs and automated processes. Further, the advent of the cyber age transformed the nature of collection from publicly available sources that open-source analysis has evolved from an information source to aid analysis to a true intelligence discipline in its own right—OSINT—with tradecraft, governance, and legal issues surrounding the collection, analysis, and production.

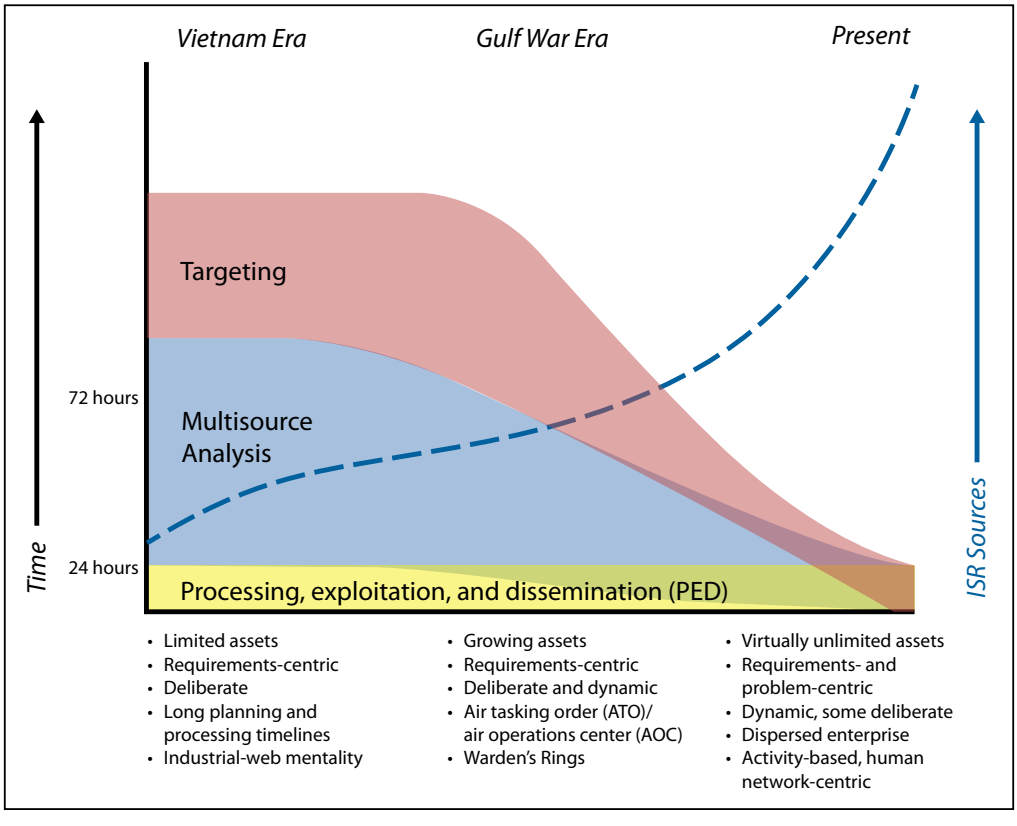

Figure 1. The information revolution's impact on collection, analysis, and targeting

The future is in data management and intelligence planning to facilitate problem-centric—rather than requirements-centric—USAF intelligence. Industrial models for production can no longer keep pace with the information environment. As National Geospatial Intelligence Agency director Robert Cardillo noted earlier this year, "If we were to attempt to manually exploit the commercial satellite imagery we expect to have over the next 20 years, we would need eight million imagery analysts. Even now, every day in just one combat theater with a single sensor, we collect the data equivalent of three NFL seasons—every game. In high definition!"[10] Analysts have more access to information than ever before and more tools at their disposal to gather information to fill gaps in knowledge. Empowering those analysts to shape the commander's knowledge of what is known, what is assessed, what is unknown, and shaping the right set of tools to answer the remaining intelligence questions is the way to get the right information to the right decision maker at the right time. Flexibility and versatility must be applied to planning and executing effects-based ISR campaigns the same way they are applied to offensive air operations.

The Four Vs and Intelligence Collection

The character of the War on Terrorism, combined with the information revolution's innovations of precision targeting, has shifted the balance of USAF efforts from the volume of ordinance dropped to the demand for ISR collection. Figure 2 illustrates the dramatic shift in balance between the aircraft and intelligence required to execute an air strike for strategic effect since World War II—with three hours of intelligence supporting 293 bombers in the 14 October 1943 Schweinfurt raid over Nazi Germany compared to more than 600 hours of intelligence work to support one 15-minute segment of a sortie in the Abu Musab al-Zarqawi raid in 2006. Precision strike requires precision intelligence, which flips the manpower burden from flying operations to processing, exploitation, and analysis to facilitate the strike operation. Recognizing the increased demand for intelligence to increase the ability to strike has resulted in a steady and sharp increase in collection platforms, sensors, and bandwidth to support "reach-back" operations, but not necessarily a commensurate increase in manpower to analyze the sheer volume of collection within the time requirements to facilitate operations. At the same time, the shift in emphasis to reach-back operations combined with the strengths and vulnerabilities of operations in the information age further muddies the historic delineation of a front and rear area of operation, rendering this concept of the operating environment an archaic notion to modern air forces.

For GEOINT, this manifested itself most visibly in an explosion in the demand for full-motion video (FMV) collection. For much of the last decade, the USAF has been awash in FMV, and it is not alone as Army organic capabilities, special operations, and partner nations press to expand the size of their fleets, increase the number of remotely piloted aircraft (RPA) sorties, and invest in the bandwidth to sustain the near insatiable demand.[11] High workloads associated with "deployed-in-place" status led the IC to steadily hollow out its workforce up to 2015, losing imagery analysts at a faster rate than they could be trained.[12] Several quality-of-life initiatives

implemented since that time reduce hours and combat the strain but also result in reduced capacity. In 2015, the USAF briefly reduced its number of RPA patrols from 65–60 to help the pilot, sensor operator, and intelligence workforce get healthy,[13] but operational realities forced the military to supplement its active duty RPA force with contractors to meet the demand.

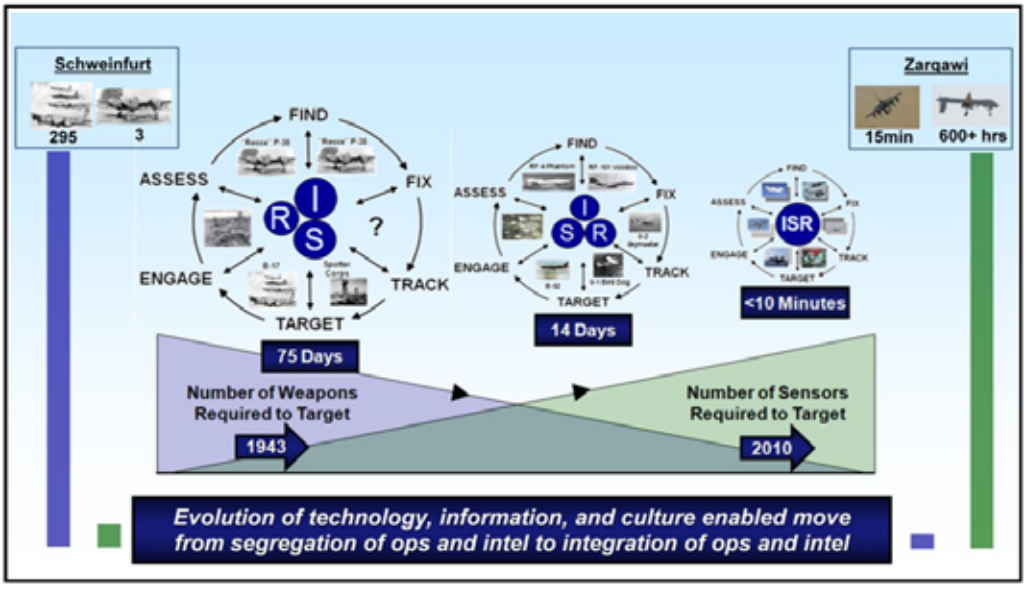

Figure 2. Implications of the information revolution for USAF targeting. (Reprinted from: Curtis E. LeMay Center for Doctrine, Development and Education, *Air Force Doctrine Document 2-0 Global Integrated Intelligence, Surveillance, and Reconnaissance Operations*, 6 January 2012, 2, https://fas.org/irp/doddir/usaf/afdd2-0.pdf.)

FMV gained the most attention outside the IC, but even within the realm of GEOINT/IMINT it represents just one source of intelligence that exploded in demand to meet operational needs. The needs for multispectral imagery, hyperspectral imagery, and ground-moving target indicator sources all continue to rise in demand across numerous operating areas;[14] including Iraq, Syria, and Afghanistan, among others. Specialized sensor suites provide the USAF with collection capabilities unrivaled in previous generations. However, those suites come with a training, manning, and time-intensive quality of analysis tail, which makes each sensor manpower intensive, straining the limited supply of imagery analysts available to process the rising collection.

The explosion of GEOINT sensors and collection capabilities introduces another significant challenge to effective analytics without the aid of big data solutions. The variety of data information collected in various graphics formats is "undiscoverable" to analysts, or what is sometimes characterized as *dark data*. Exploited GEOINT generally has textual summaries that can be searched, through queries similar to a Google image search, but absent text to cue the analyst, the relevant imagery may remain buried and undiscoverable in data archives. Big-data algorithms and automated

exploitation templates can allow all images, in NRT, to be tied to geographic coordinates, aligned to known locations, and automatically archived in searchable layered databases with related images over time. While the current model for ISR is operations-centric, requiring new sorties to gather geospatial information (particularly for problem sets like pattern-of-life), big-data analytics will provide future analysts access to a library of historical data and the tools to rapidly sift through potentially thousands of images to see changes over time and analyze the significance.

GEOINT is not alone in seeing an exponential increase in demand for collection and analysis. The increase in collection platforms also led to an increase in collector payloads across intelligence disciplines, including SIGINT payloads. As the number of collection opportunities rises, and as global connectivity rises in the information age with global-networked threats emerging, the volume, velocity, and variety of signals collected continue to rise, often at a rate faster than our ability to recruit and train analysts.[15] Just as hours of video acquired by RPAs may go unanalyzed for years without the prospect of big-data analytics to aid in cueing analysts to key segments of analysis collection, hours of intercepted communications may go without being analyzed absent automated tools to sort through the petabytes of collection. Beyond SIGINT and GEOINT, MASINT has similarly seen a boom in both collections and demand for production, with synthetic aperture radar and coherent change detection, among other capabilities in increasingly high demand.[16]

Open-source Intelligence

Perhaps no example illustrates the sea change of collection regarding the four Vs of big data more than the creation of OSINT as a true intelligence discipline. When we say OSINT is a new discipline, many Cold War-era analysts will caution, "No, we've always had OSINT, and the Central Intelligence Agency's (CIA) Open Source Center is proof."[17] Indeed, a common rule of thumb cited for decades, dating to a statement from then-CIA Director Allen Dulles, is that more than 80 percent of intelligence analysis is ultimately derived from open source. All this is true, but it would doctrinally be better characterized as *open-source information*. OSINT as an intelligence discipline is directly tied to the proliferation of the internet and social media, and with it the need to develop new tradecraft for search and discovery of information, oversight to ensure relevant laws and orders protecting citizens and safeguarding information are observed by the IC, and governance of the process. Absent big-data analytic solutions, it would be impossible for analysts to sort through the billions of data points available (volume, variety, and velocity), identify the relevant and irrelevant pieces of data (veracity), safeguard the rights of citizens and follow other applicable laws and regulations, and discover relevant intelligence insights to meet customer needs.

The information revolution led to a new online culture of sharing, and what many characterize as oversharing.[18] The upside for the IC is that through Twitter, Facebook, Snapchat, blogs, and numerous social media sites not even invented yet, intelligence has access to tens of millions of passive collectors all over the world. In the 1990s, analysts faced the prospect that battle damage assessment might be

conducted on CNN before they had time to complete the intelligence cycle for assessment. Today, if an RPA loses connectivity and crashes, it is likely to be reported on Twitter and retweeted multiple times before the aircraft is confirmed lost. Academic research and intelligence analysis now rely on sentiment analysis, in essence, a sophisticated and tailorable version of "trending" on Twitter, to determine the sentiments of populations as a potential predictor of future activity (civil unrest, and so forth).

Time Demands of Operations

In most commercial discussions of big data, velocity focuses on how rapidly information is acquired. For intelligence operations, velocity can equally apply to how rapidly operators, commanders, and other decision makers require intelligence outputs to facilitate operations. The campaign against the Islamic State has been for the United States predominantly an air-centric campaign, emphasizing both deliberate and dynamic targeting to isolate and degrade a proto-state with limited fixed infrastructure and which readily blends into the population for defense from strikes.[19] This combination, along with the necessity to minimize the risk of collateral damage, has only served to add to the demands for ISR. This includes both finding and characterizing targets, maintaining overwatch of potential targeted locations, and understanding patterns of life among the population. Lt Gen Charles Q. Brown Jr., the coalition forces air component commander, made the point explicit in May 2016, stating, "Because what it helps me to do is develop targets so we can strike at the same time as we develop those targets. The more ISR I have, I can minimize the risk to civilian casualties and continue the precision air campaign that we have."[20]

More in this context has both volume and time dimensions as the time the information will be of value in a dynamic strike is minimal, especially compared to a more traditional target such as an airfield, a command bunker, or a portion of a communications network. The NRT nature of FMV and its critical role in the engagement/finish phase of operations led many observers to conclude targeting is easier to do today in real time, but in practice this represents the tip of the intelligence iceberg that facilitated the strike. Coalition forces require a globally synchronized network of analysts to rapidly fuse imagery, electronic intercepts, and tips from informants to cue potential targets for a strike. Globally-integrated ISR facilitates these networks via timely access to more collection but with it a significant veracity problem. At the same time, this system is simultaneously raising critiques from human rights organizations with civilian casualties concerns and from advocates of more traditional air campaigns that the overall numbers of targets being struck are insufficient even by the standards of recent campaigns.[21] The ISR community, and the IC more broadly, must face the complex management problem of distributed operations, quality control of analysis, and management of data sets to give both the ISR enterprise and operators acting in real-time full visibility to target development progress.

The Threat Environment

The Islamic State in Iraq and Syria's (ISIS) regular appeals to "lone wolf" terrorism through what has been called the *digital caliphate* highlights the challenge the internet poses to security in the West.[22] Before that, cyber collectives like 4chan/"Anonymous" were exploiting online connectivity to build anarchic communities of information sharing that ultimately facilitated collective action on a number of issues.[23] As US military intelligence has traditionally regarded conventional military dominance as the focal point of its mission, in the information age weaponized narrative is rapidly gaining focus as a theater of operations for national security.[24] Understanding the threat environment in the information era will only be possible with access to, and the effective utilization of, big data solutions. While countering this challenge will likely ultimately fall to non-DOD entities such as the State Department, the USAF's mission demands awareness and defense of the cyber domain. As such, USAF intelligence analysts must be at the forefront of analyzing and discovering threats in the cyber domain.

The past decade of counterterrorism and counterinsurgency operations has made USAF intelligence analysts well-versed in monitoring and evaluating terrorist networks in conflict zones, particularly in Iraq as was the case with al-Qaeda in Iraq and with Taliban-linked groups in Afghanistan. Cyber collectives represent a distinct challenge, however. Cyber collectives lack a centralized command structure, instead operating largely through online community norms and values. Their membership is open, without formal recruitment or retention mechanisms, and their strategic planning is minimal. Most tend to resist anyone emerging as a leader or spokesperson for their group; influencers might emerge for limited periods, but the open and diverse nature of membership prevents anyone from emerging for an extended period without fracturing the group. Smaller communities might develop stronger internal hierarchies as limited membership brings with it homogenous ideologies, but this serves to limit the global reach and influence of larger collectives.[25] Figure 3 illustrates the distinctions in brief between a hierarchy, a network, and cyber collectives.

The character of intelligence collectives provides a forum that can be infiltrated to spark lone wolf or wolfpack attacks; information simultaneously spread among a circle of the collective initiates an action —think a flash mob—with little to no warning. At the same time, the anarchic character of collectives tends to make their justifications anarchic as well; their *modus operandi* is often to oppose authority figures and abuses of power, not to actively seek to replace it with a new dominant ideology. For this reason, many lone wolf and wolfpack strikes launched by individuals recruited through collectives, even when inspired by organizations with specific ideologies, do not necessarily show an affinity for specific ideological positions; only their reactionary nature. As one example, Orlando nightclub shooter Omar Mateen may not have understood the difference between ISIS, al-Qaeda, and Hezbollah, despite there being significant sectarian and strategic distinctions between these groups.[26] In line with the characteristics of cyber collectives, however, these groups are linked online by anti-Western sentiments and an anarchic perspective toward the Western order. Calls to incite chaos to avenge moral wrongs propagate in

that environment, while specific ideological messages and more formal alignments with specific groups may not.

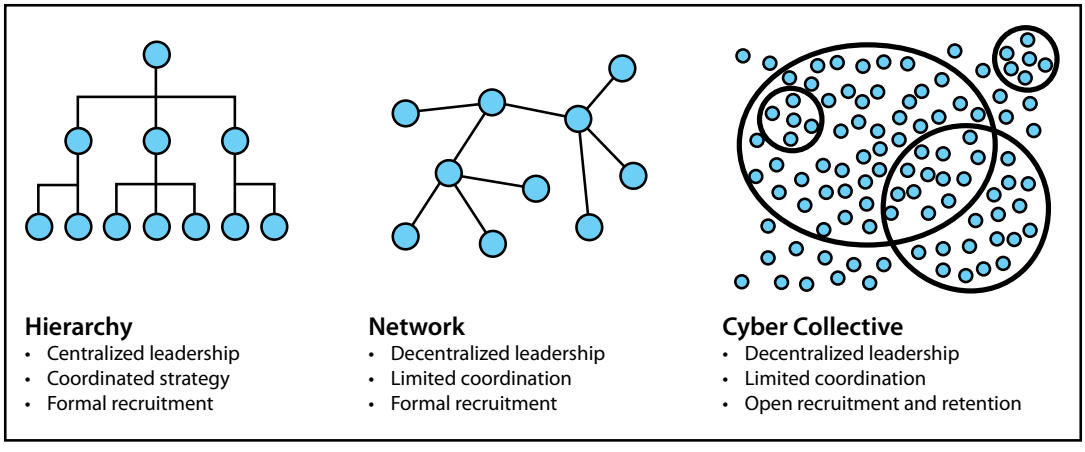

Figure 3. Hierarchies, networks, and cyber collectives. (Derived from sourcing in Max Sterling, "The Cyber Collective Threat: A Pack of Lone Wolf Terrorists," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary,* April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf.)

The challenge for intelligence agencies stemming from this new decentralized organization is the prospect of infiltration of collectives as part of a multipronged strategy aimed simultaneously as destabilizing adversaries through deep state attacks while concentrating more organized and strategic violence against local governments through both networked and hierarchic organizations.[27] Figure 4 illustrates how this hybrid model might look, with a central strategic leadership core directing actions across multiple departments for recruitment, propaganda, training, direct action operations, coordination with networks, and online propaganda infiltration of cyber collectives. As broad and diverse as these networks are, traditional network mapping is not possible given how rapidly they can shift and how fast messages can be shared through collectives. Identifying influencers within the network requires big-data solutions to follow volume of message traffic, identify what themes might be trending and what messages might be receptive in what areas, and to identify shifts in trends in those messages which might presage a change in attack strategies (mass shootings, crashing vehicles, and the next evolution of threats). This level of understanding of adversary organizations and messaging is vital to countering adversaries directly at the operational level and above, but potentially more importantly for tactical indications and warnings for force protection.

Just as adversaries can use the cyber domain to carry out operations through influence, they can use cyber tools to thwart intelligence and to amplify their messages. One of the most prominent today is the use of bots;[28] software robots designed to automatically propagate messages via social media and other online venues. These can distort data for sentiment analysis, sway public opinion through a bandwagon effect by making it appear more popular, automatically spread disinformation

through cyber collectives, and to amplify recruitment. Investigations of Russia's potential activities in the 2016 election have focused not so much from the threat of hacking in the traditional sense, but social engineering executed by bots with messages aimed at specific groups.[29] Going forward, analysts operating in a complex multidomain environment must understand the emerging nature of threats posed by the cyber realm.[30] Maintaining basic situation awareness, much less gaining operational understanding, can only come through a better understanding of big-data analytics and recognition of both its power as a tool and its vulnerabilities.

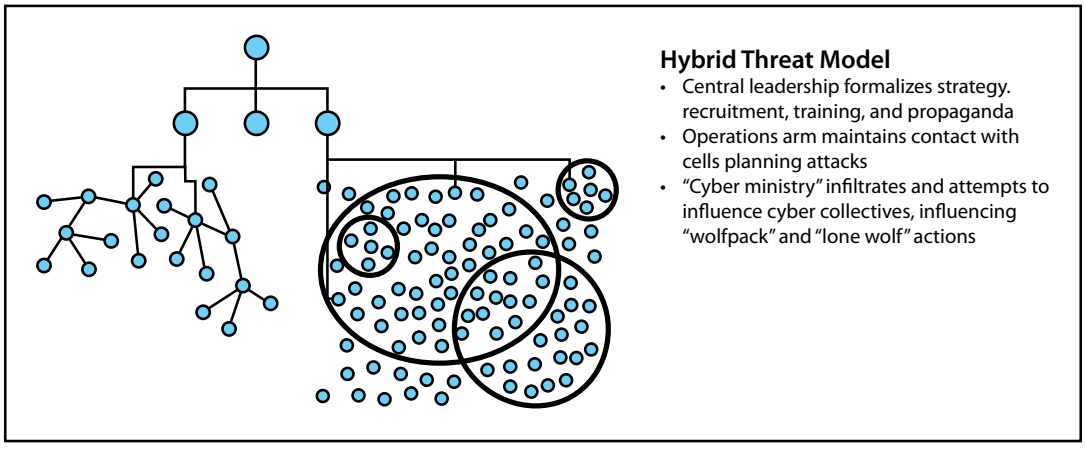

Figure 4. The hybrid threat of infiltrated cyber collectives

The Industrial Age Intelligence Model versus the Information Age Model

The three Vs of big data, combined with their implications for friend and foe alike, necessitate a rethinking of our industrial model for intelligence production. All intelligence operators are trained from their basic courses in the five-step intelligence cycle known as planning and direction; collection; processing, exploitation, and dissemination (PED); analysis and production; and dissemination (PCPAD).[31] This structured and repeatable process ensures clarity of the steps of production and provides checks and balances over analytical processes. It also contains bureaucratic elements, particularly for large organizations such as USAF intelligence that correlate steps of the PCPAD cycle with different units/offices. An information age model of intelligence must find ways to move beyond the bureaucratic model alone (not replace it, but supplement it), and facilitate data management across a distributed enterprise to support decision-quality intelligence for operational demands. Data science must be viewed as a core competency of the intelligence community in the information age, and traditional intelligence analysts must work hand-in-hand with skilled computer scientists and data managers to facilitate intelligence production.

Another challenge/opportunity for USAF intelligence is the conflation of intelligence and ISR. The DOD defines ISR as "an activity that synchronizes and integrates

the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function."[32] Although it is a combination of intelligence and operations, it represents a subset of the overall intelligence cycle. Tasking represents the final portion of the planning process, where units are assigned requirements through the ATO, while collection and PED mirror those stages of the PCPAD cycle, as illustrated in figure 5.

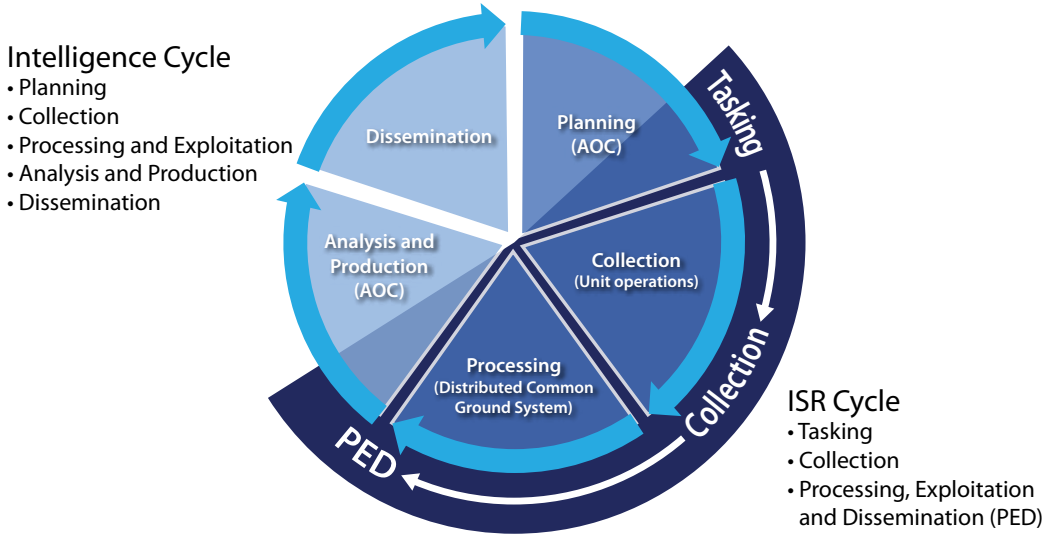

Figure 5. Industrial model of intelligence production

This model sets up an infrastructure for intelligence analysis that proved effective in evaluating state actors, but its time-sequenced character has in practice placed a limiting factor on the USAF's ISR OODA loop. ISR planning is executed through the 72-hour ATO tasking cycle and is governed by a collection management process whereby commanders' priorities for collection targets (sites to be imaged or otherwise collected) are racked and stacked through a boarded or refereed prioritization process before ATO execution. This is followed by an analysis process which can add days to the process for operational-level analysis within the USAF, or weeks for all-source production at national agencies. This interferes from an ISR standpoint with the USAF principle of flexibility, which should enable ISR operators to mass and maneuver ISR effects to critical points in the operating environment for integration in time, space, and purpose.[33] Further, as ISR sources have grown more complex and the stockpile of underlying intelligence data and information grows, it is unlikely that traditional models for developing priority intelligence requirements, commander's critical information requirements, and other intelligence collection requests in the future will remain an efficient means of prioritizing collection assets.

In the mid-2000s, ISR operators faced the challenge of explaining to customers, "Don't request an asset like Predator; request a capability like FMV." Today, the

problem is compounded as collection sources are much more specialized and numerous, leaving ISR tacticians best positioned to determine which ISR source is best positioned to fill an intelligence gap. Adding passive sensors like OSINT and discoverable big-data analysis of existing HUMINT, SIGINT, GEOINT, and MASINT data may rapidly answer a customer perceived problem absent the need for additional collection to a confidence level sufficient to justify not retasking the asset. While the vast majority of assets and collection allocations will, for the immediate future, continue to be tasked through this standard process, a share of airborne ISR assets and analytic capability must be dedicated to an information age alternative to directly shape the air campaign in NRT.

The alternative for the information age is problem-centric intelligence, spearheaded by an ISR task force. Rather than tasking collection, the operations input to the ISR process should be perceived intelligence problems, which ISR specialists can then translate to refined ISR problems, intelligence gaps, and prioritize ISR sensors in a combined scheme of maneuver to fill those gaps. An ISR task force, empowered by a single commander with organic collection requirements management and collection operations management authorities, is empowered to build an integrated ISR plan for a specified operational objective. This is the next step in the advancement of USAF Central Command's 2009 directive codifying ISR mission-type orders (MTO) as critical to supporting operational contingency operations.[34] Absent a specified ISR task force with ownership of ISR assets and authority to task them, the current MTO construct is more akin to an ISR coordination card for retasking than a true mission type order as defined in Joint Publication 3-50, *Personnel Recovery*.

This ISR task force model, outlined in figure 6, restructures the planning process for organic airborne ISR assets to a problem-centric mold, incorporating big-data analytics to refine the tasked ISR problem. The "IC Cloud," composed of access to NRT OSINT data and the full database of multi-INT analysis from across the IC, allows analysts in the earliest stages of the process to shape answers to the customer's problem, while refining their intelligence questions based on a refined understanding of what is actually known by the IC. ISR tacticians can then match the best collection platform to answer the intelligence gap. ISR operations can then be readily retasked by the ISR task force, under the authority of the commander through the intent of the MTO; in practice by a designated operator with sensor tasking authority. This provides NRT refinement of collection in concert with PED and fusion entities, maximizing the utility of the sensor. ISR task force products can then be distributed in NRT simultaneously to operational customers for planning and targeting decisions and to the larger IC for further analysis and ultimately incorporation into the IC Cloud for future exploitation.

Enabling this big-data solution to intelligence analysis and ISR tasking also requires the USAF intelligence community to think bigger about its personnel choices moving forward, as depicted in figure 6. The IC to date has accepted specialists in a number of scientific fields beyond intelligence officers and enlisted personnel. To make big data work in the future, the USAF intelligence enterprise must incorporate data scientists, computer programmers, and social scientists with expertise in the cyber domain to comprehend the nature of the data we access, and effectively analyze the operating environment of the cyber domain.

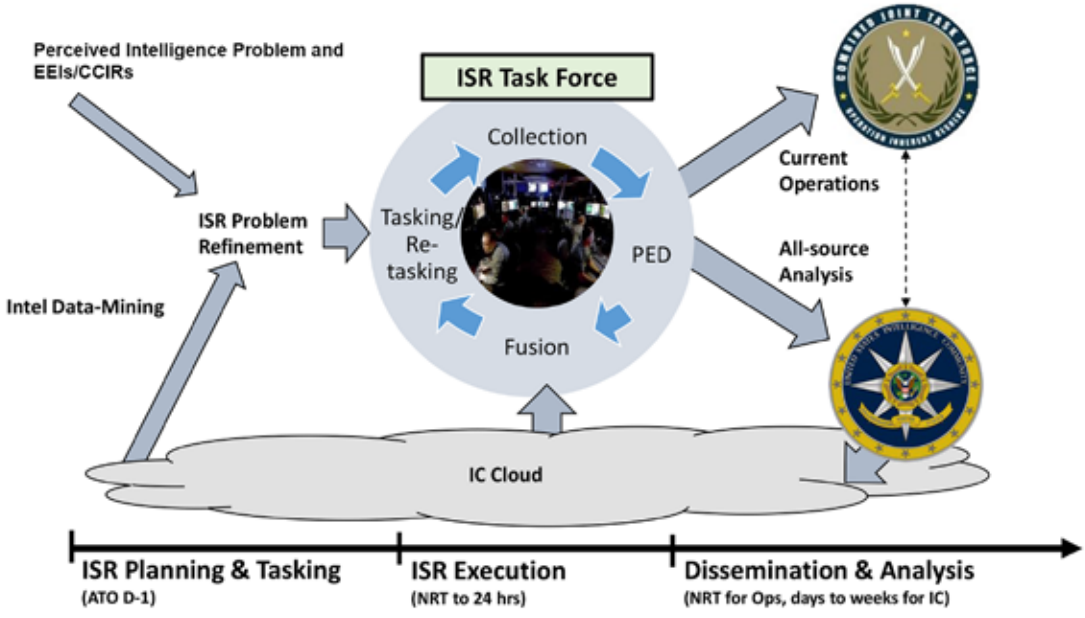

Figure 6. Intelligence, surveillance, and reconnaissance task force model for airborne intelligence. (Source: Maj Michael P. Kreuzer and Maj Denis A. Dallaire, "Targeting the Islamic State," The Mitchell Institute for Aerospace Studies, 14 April 2017, http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf.)

Conclusion

To paraphrase an old quote, you may not be interested in big data, but big data is interested in you.[35] Big data shapes the modern information environment, and through information sharing and access to the cloud, big data is already radically restructuring how analysts access and interpret data. Adversaries exploit the complex cyber environment to recruit, influence populations, and execute attacks against US interests in a manner that can only be detected through big-data solutions. Our ability to collect and store raw data continues to exceed our ability to process what we have collected, meaning we likely already have, somewhere in our vast databases of information, the answers to the puzzles intelligence customers have today and the ones they will pose tomorrow. Absent big-data solutions to manage the data and information we continue to collect and bring it to ISR planners rapidly to facilitate smarter, timely collection, the USAF intelligence community will face information overload resulting in decision paralysis. Getting the right information to the right customer at the right time means rethinking ISR planning, and embracing big-data solutions to the ISR challenges we face. ✪

Notes

1. David Rotman, "How Technology Is Destroying Jobs," *MIT Technology Review*, 12 June 2012, https://www.technologyreview.com/s/515926/how-technology-is-destroying-jobs/; Zeynep Tufekci, "The Machines are Coming," *New York Times*, 18 April 2015, https://www.nytimes.com/2015/04/19/opinion/sunday/the-machines-are-coming.html?_r=0; Dirk Helbing, Bruno S. Frey, Gerd Gigerenzer, Ernst Hafen, Michael Hagner, Yvonne Hofstetter, Jeroen van den Hoven, Roberto V. Zacari, Andrej Zwitter, "Will Democracy Survive Big Data and Artificial Intelligence?," *Scientific American*, 25 February 2017, https://www.scientificamerican.com/article/will-democracy-survive-big-data-and-artificial-intelligence/; and Tim Harford, "Big Data: Are We Making a Big Mistake?," *Financial Times*, 28 March 2014, https://www.ft.com/content/21a6e7d8-b479-11e3-a09a-00144feabdc0.

2. SAS Institute, "Big Data: What It Is and Why It Matters," 24 May 2017, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html.

3. Richard Holt, "Twitter in Numbers," *Telegraph*, 21 March 2013, http://www.telegraph.co.uk/technology/twitter/9945505/Twitter-in-numbers.html.

4. SAS Institute, "Big Data Analytics."

5. Geethika B. Peddibhotla, "Gartner 2015 Hype Cycle: Big Data is Out, Machine Learning is in," *KD Nuggets*, http://www.kdnuggets.com/2015/08/gartner-2015-hype-cycle-big-data-is-out-machine-learning-is-in.html.

6. Harford, "Big Data."

7. SAS Institute, "Machine Learning: What It is and Why It Matters," 24 May 2017, https://www.sas.com/en_us/insights/analytics/machine-learning.html.

8. Office of the Director of National Intelligence, "What is Intelligence?," 24 May 2017, https://www.dni.gov/index.php/what-we-do/what-is-intelligence.

9. Developed by John Boyd in the 1950s and introduced to Air Force training in the 1960s and 1970s, the "OODA Loop" (observe, orient, decide, and act) represents one model for decision making across four phases with the implication that a faster and better OODA Loop than your opponent is essential to gaining an advantage in combat. For a brief example, *see* Richard Feloni and Anaele Pelisson, "A Retired Marine and Elite Fighter Pilot Breaks Down the OODA Loop, the Military Decision-making Process that Guides 'Every Single Thing' in Life," *Business Insider*, 13 August 2017, http://www.businessinsider.com/ooda-loop-decision-making-2017-8.

10. Robert Cardillo, "National Geospatial Intelligence Agency (NGIA) *2017* Symposium Remarks," (lecture, NGIA Headquarters, Springfield, VA, 5 June 2017), https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx.

11. Christopher Drew, "Military Is Awash in Data from Drones," *New York Times*, 10 January 2010, http://www.nytimes.com/2010/01/11/business/11drone.html; Kevin McCaney, "Pentagon Plans to Boost Drone Flights by 50 Percent," *Defense Systems*, 17 August 2015, https://defensesystems.com/articles/2015/08/17/pentagon-to-increase-drone-flights-50-percent.aspx; and Julian E. Barnes, "NATO Invests in More Bandwidth for New Data-Hungry Drones," *Wall Street Journal*, 27 March 2017, https://www.wsj.com/articles/nato-invests-in-more-bandwidth-for-new-data-hungry-drones-1490601588.

12. Pratrap Chatterjee, "The Side of Drone Warfare No One Is Talking About," *Nation*, 13 July 2015, https://www.thenation.com/article/the-side-of-drone-warfare-no-one-is-talking-about/.

13. Marcus Weisgerber, "Air Force Trims Drone Ops to Get Workforce 'Healthy,'" *Defense One*, 18 May 2015, http://www.defenseone.com/business/2015/05/air-force-trims-drone-ops-workforce-healthy/113122/.

14. Joey Cheng, "Hyperspectral Sensor Lets Drones See through Camouflage, Spot Explosives," *Defense Systems*, 25 February 2015, https://defensesystems.com/articles/2014/02/25/air-force-aces-hy-hyperspectral.aspx?admgarea=DS.

15. National Security Agency (NSA), "Signals Intelligence," *NSA*, 24 May 2017, https://www.nsa.gov/what-we-do/signals-intelligence/.

16. "RQ-4A/B Global Hawk HALE Reconnaissance UAV, United States of America," *Air Force Technology*, 24 May 2017, http://www.airforce-technology.com/projects/rq4-global-hawk-uav/rq4-global-hawk-uav6.html.

17. Central Intelligence Agency (CIA), "Open Source Center," *CIA*, 24 May 2017, https://www.cia.gov/careers/games-information/view-our-advertising/pdf/OSC%20Insert.pdf.

18. Mary D. Harrington, and Lisa E. Heffernan, "Oversharing: Why Do We Do It and How Do We Stop?," *Huffington Post*, 3 February 2014, http://www.huffingtonpost.com/grown-and-flown/oversharing-why-do-we-do-it-and-how-do-we-stop_b_4378997.html.

19. Maj Michael P. Kreuzer and Maj Denis A. Dallaire, "Targeting the Islamic State," *The Mitchell Institute for Aerospace Studies*, 14 April 2017, http://docs.wixstatic.com/ugd/a2dd91_4892807f169341188b7ebcd2f775671d.pdf; and Dave Majumdar, "Pentagon: ISIS Adapting to Air Strikes, Targeting Becoming 'More Difficult,' " *USNI News*, 11 August 2014, https://news.usni.org/2014/08/11/pentagon-isis-adapting-air-strikes-targeting-becoming-difficult.

20. Kristina Wong, "US Commander: Lack of Intelligence Assets Slowing Down ISIS War," *Hill*, 7 June 2016, http://thehill.com/policy/defense/282457-isis-air-war-commander-short-on-intelligence-assets.

21. Eric Schmitt, "U.S. Says Its Strikes Are Hitting More Significant ISIS Targets," *New York Times*, 25 May 2016, https://www.nytimes.com/2016/05/26/us/politics/us-strikes-isis-targets.html?_r=0.

22. Haroon Ullah, "Taking on the 'Digital Caliphate' in Our Fight Against ISIS," DIPNOTE: *US Department of State Official Blog*, 27 March 2017, https://blogs.state.gov/stories/2017/03/27/en/taking-digital-caliphate-our-fight-against-isis.

23. Max Sterling, "The Cyber Collective Threat: A Pack of Lone Wolf Terrorists," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary*, April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Sterling.Max.pdf; and Dale Beran, "4chan: The Skeleton Key to the Rise of Trump," *Medium*, 14 February 2017, https://medium.com/@DaleBeran/4chan-the-skeleton-key-to-the-rise-of-trump-624e7cb798cb.

24. Brad Allenby, "Weaponized Narrative is the New Battlespace," *Defense One*, 3 January 2017, http://cdn.defenseone.com/b/defenseone/interstitial.html?v=7.5.0&rf=http%3A%2F%2Fwww.defenseone.com%2Fideas%2F2017%2F01%2Fweaponized-narrative-new-battlespace%2F134284%2F%3Foref%3DDefenseOneFB.

25. Sterling, "Cyber Collective Threat."

26. Adam Taylor, "Omar Mateen May Not Have Understood the Difference between ISIS, al-Qaeda and Hezbollah," *Washington Post*, 13 June 2016, https://www.washingtonpost.com/news/worldviews/wp/2016/06/13/omar-mateen-may-not-have-understood-the-difference-between-isis-al-qaeda-and-hezbollah/?utm_term=.4718e23fe6f5.

27. Charlie Winter, "What I Learned from Reading the Islamic State's Propaganda Instruction Manual," *Lawfare*, 2 April 2017, https://www.lawfareblog.com/what-i-learned-reading-islamic-states-propaganda-instruction-manual.

28. Matthew Bondy, "Bad Bots," *The Project on International Peace and Security, Institute for the Theory and Practice of International Relations, College of William and Mary*, April 2017, http://www.wm.edu/offices/itpir/projects/pips/_documents/pips/2016-2017/Bondy.Matthew.pdf.

29. Gabe O'Connor, "How Russian Twitter Bots Pumped Out Fake News During The 2016 Election," *NPR*, 3 April 2017, http://www.npr.org/sections/alltechconsidered/2017/04/03/522503844/how-russian-twitter-bots-pumped-out-fake-news-during-the-2016-election.

30. Tech Sgt Robert Barnett, "Goldfein: Future of War is Networked, Multi-domain," *US Air Forces Central Command*, 22 March 2017, http://www.afcent.af.mil/News/Article/1127569/goldfein-future-of-war-is-networked-multi-domain/.

31. CIA, "The Intelligence Cycle," *CIA*, 24 May 2017, https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html.

32. The Joint Staff, *DOD Dictionary of Military and Associated Terms*, 118, March 2017, http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf.

33. Curtis E. LeMay Center for Doctrine, Development and Education, *Volume 1, Basic Doctrine: Flexibility and Versatility*, 27 February 2015, https://doctrine.af.mil/download.jsp?filename=V1-D82-Flexibility-Versatility.pdf.

34. Capt Jaylan M. Haley, "An Evolution in Intelligence Doctrine: The Intelligence, Surveillance, and Reconnaissance Mission Type Order," *Air & Space Power Journal*, October 2012, http://www.airuniversity.af.mil/Portals/10/ASPJ/journals/Volume-26_Issue-5/ASPJ-Sept-Oct-2012.pdf.

35. Ken Blackwell and Bob Morrison, "Like It or Not, War Is Interested in You," *American Thinker*, 23 April 2013, http://www.americanthinker.com/articles/2013/04/like_it_or_not_war_is_interested_in_you.html.

Col Shane P. Hamilton, USAF

Colonel Hamilton (MS, USAFA; MS, School of Advanced Air and Space Studies (SAASS), Embry-Riddle Aeronautical University; MS, Industrial College of the Armed Forces) is the deputy director of intelligence, Headquarters Air Combat Command (ACC). He has commanded at the squadron and group levels, led Joint Intelligence Fusion for US Forces Korea, and most recently served as ACC's director for the Intelligence Analysis, Targeting, and Collection Management Directorate. He is a graduate of the USAF Weapons School and the SAASS.

Lt Col Michael P. Kreuzer, USAF, PhD

Lieutenant Colonel Kreuzer (BA, USAFA; PhD, Princeton University; MPA, University of Alaska–Anchorage; MSI, American Military University) is the executive officer, ACC Directorate of Intelligence. He is a career intelligence officer who has served as director of special programs in counter-improvised explosive devices and collection management for Multinational Division North in Iraq, the intelligence staff officer of the Kapisa Provincial Reconstruction Team in Afghanistan, and chief of USAF Intelligence Officer Formal Training.

Distribution A: Approved for public release; distribution unlimited.

http://www.airuniversity.af.mil/ASPJ/