REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
23-03-2017	Master of Military Studies Research Paper	September 2016 - April 2017

4. TITLE AND SUBTITLE

Improving Intelligence Analysis via Automated Information Processing and a Correlation Analytic Mindset

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)

Wetzel, Tyson K., Major, USAF

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSOR/MONITOR'S ACRONYM(S)
N/A

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

N/A

14. ABSTRACT

The explosion of intelligence collection platforms and sensors, and the general explosion in data are overwhelming current information processing tools, creating a data overload problem. Analysts are unable to manually access, fuse, and analyze all available data, hurting the quality of assessments provided to commanders and decision-makers. Automated processing tools promise to leverage “big data." However, analysts are not taught what “big data” is, how to use automated processing tools, or how analysis will change in a big data world. This paper argues for a change in the intelligence analysis mindset from inferred causality to data-driven correlations that enable predictive intelligence assessments.

15. SUBJECT TERMS

Intelligence, ISR, big data, analysis, near-peer conflict

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Marine Corps University/Command and Staff Col
Unclass	Unclass	Unclass	UU	38	19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

TITLE: Improving Intelligence Analysis via Automated Information Processing and a Correlation Analytic Mindset

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF MILITARY STUDIES

AUTHOR: Major Tyson K. Wetzel, USAF

AY 16-17

Mentor and Oral Defense Committee Member: Dr. Douglas G. Stronsand
Approved: [signature]
Date: 7 April 2017

Oral Defense Committee Member: Lt Col Mark D. Howard
Approved: [signature]
Date: 7 April 2017

Executive Summary

Title: Improving Intelligence Analysis via Automated Information Processing and a Correlation Analytic Mindset.

Author: Major Tyson Wetzel, United States Air Force

Thesis: In order to improve intelligence assessments, military intelligence analysts must exploit current and developmental automated information processing tools, and focus on data-driven, correlation-focused assessments to improve current warfighting and prepare for possible future "near-peer conflicts."

Discussion: The explosion of intelligence collection platforms and sensors, and the general explosion in data are overwhelming current military intelligence information processing tools, creating a data overload problem. Analysts are unable to manually access, correlate, fuse, and ultimately analyze all available data, hurting the quality of intelligence assessments provided to operational commanders and civilian decision makers. Automated information processing tools promise to leverage "big data" and make intelligence collection much more accessible to the intelligence analyst. However, intelligence professionals are not being taught what "big data" is, how to use automated information processing tools, or how intelligence analysis will change in a data-driven world. This paper will not advocate for a specific software tool, but will instead argue for a change in the intelligence analysis mindset from conclusions derived from inferred causality based off of limited information, to data-driven correlations that enable predictive intelligence assessments.

Conclusion: Mastering the use of big data may give the US a generational advantage over their adversaries in providing more complete, timely, and accurate inputs that inform and quicken the tempo of our OODA Loop, and provide our military forces an asymmetric advantage on the battlefield.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Page

Preface

For years I have been hearing about something called "big data," and how it will revolutionize military intelligence. As I learned more about big data I realized most who were talking about it knew very little about the concept, and instead used it as a catchphrase. As a Director of Operations of an intelligence squadron, I saw first-hand the inefficiency of the manual intelligence process. I wanted my Airmen to have automated tools that would access, correlate, and fuse data, allowing them to focus on making timely and actionable assessments for our operational commanders. I have heard promises from a plethora of defense contractors and organizations that they are building the software tools that will leverage the awesome power of big data. Though I remain somewhat skeptical, I realized our intelligence professionals are not trained on how to use big data and automation tools. My desire to prepare our analysts for the big data world was the genesis of this paper. Though heavily weighted towards Air Force sources, this paper is not service specific; rather it is a guide for all analysts to prepare for using big data.

Dr. Douglas Streusand has been a mentor and guide throughout the process, providing focus and scope to this paper. In my career I have been lucky enough to serve with and for some of the most creative and innovative minds in the Air Force intelligence career field, and each has inspired me to "think differently" about intelligence analysis. Lieutenant Generals Jack Shanahan and Veralinn "Dash" Jamieson are sueprbly leading Air Force Intelligence, while Brigadier General Tim Haugh and Colonel Jason Brown are working tirelessly to provide the tools to our Airmen, encouraging the type of innovative thinking that will ensure our intelligence professionals stay ahead of our adversaries. Last and certainly not least, Lieutenant Colonel Amanda Figueroa inspires me as a brilliant commander, an invaluable editor, and an amazing wife; none of my achievements would be possible without her.

Table of Contents

The recent development of new sensors and methods of intelligence collection has vastly increased the amount of data available to military intelligence analysts. However, automated software tools have not kept pace with the explosion of available data. Military intelligence analysts must manually correlate, fuse, and analyze available data.[1] The explosion of data and the inadequacy of automated information processing tools present three major problems for the intelligence analyst. First, intelligence professionals make assessments from data they have the capacity to manually fuse and analyze; meaning much of the available data is not utilized. Second, manual processing and data fusing cause analysts to miss critical relationships and correlations.[2] Finally, analysts tend to focus on identifying causal linkages and frequently err in doing so, resulting in poor intelligence assessments. The most frequent analytical error is sometimes called the "post hoc ergo propter hoc" problem;[3] analysts tend to assume an event was caused by a given input simply because the result happened after the input. In order to improve intelligence assessments, military intelligence analysts must exploit current and developmental automated information processing tools, and focus on data-driven, correlation-focused assessments to improve current warfighting and prepare for possible future "near-peer conflicts."

In order to take full advantage of automated information processing tools, analysts must shift their emphasis from inferring causal linkages to identifying data-driven correlations. The

[1] See Appendix A: *Joint Military Definitions and Terms* for joint service definitions of each of these terms.
[2] According to Joint Publication 2-0, *Joint Intelligence* (22 October 2013), the six categories of intelligence operations are: 1) planning and direction; 2) collection; 3) processing and exploitation; 4) analysis and production; 5) dissemination and integration; 6) evaluation and feedback (pp. x). "Data conversion and correlation" occur within the processing and exploitation phase of the intelligence cycle (pp. I-15). See Appendix B: *The Intelligence Process* for a graphical depiction of the process. Unfortunately, joint doctrine does not define "correlation." However, the Merriam-Webster online (www.merriam-webster.com/dictionary/correlation) definition of correlation: "the relationship between things that happen or change together," accurately represents the contextual use of "correlation" in JP 2-0. When discussing correlation in the intelligence process the Merriam-Webster definition will be used in this paper, though an alternate, data-focused definition of the term will be introduced later.
[3] Latin for "after this, therefore resulting from it." The phrase is often used as an example of a logical bias or fallacy.

purpose of this paper is not to advocate for a specific technology or software, but to advocate for the use of automated information processing tools to enable intelligence professionals to automatically filter, fuse, and correlate huge amounts of data, as well as to improve the analysis of that data. This paper will advocate not only the use of automated information processing systems and its resulting data-driven assessments (frequently referred to holistically as "big data analytics"), but also a shift in analytic mindset from inferred causation to data-driven correlation in the development of intelligence assessments.

This paper will guide intelligence professionals in their use of automated information processing systems and how to think about correlation in a big data world. It will also provide commanders with a framework for interpreting intelligence assessments based on big data. Part I will begin by examining the explosion of data and the implications of the "data overload problem" on military intelligence analysis. Part II will explore the concept of "big data" and examine the potential benefits of automated information processing tools. Part III will expound upon the need for a mind-set shift among intelligence analysts to use automated information processing tools effectively. Part IV, broken into two sections, will explain how this new analytic mindset will aid intelligence producers and consumers across the range of military operations. Section 1 will introduce the phenomenon of an individual or a unit's "digital trail," and how intelligence analysts in various mission types or against various target types can use that digital trail. Section 2 will use a case study to apply automated information processing tools and a correlation analytic mindset to a modern military problem, finding a mobile surface-to-air missile (SAM) battery. Part V is the conclusion and will focus on how intelligence professionals and military commanders should use data-driven intelligence conclusions and assessments.

Part I: The Data Overload Problem

The data overload problem refers to the risk of prodigious amounts of data overwhelming a person or organization's ability to use it. This problem is magnified in the intelligence profession for three primary reasons; the information revolution has massively increased the amount of available data, which threatens to overwhelm current information processing systems; current information processing systems are not integrated among the military services, intergovernmental agencies, and international partners; and manual information processing is time consuming, inefficient, and ineffective. The data overload problem results in the three major intelligence analysis problems outlined in the introduction; analysts must rely on manual information processing, limiting their total data management capacity; the limited amount of data able to be manually processed frequently results in missed correlations and relationships; and manual information processing forces intelligence assessments to be developed using incomplete data, causing analysts to erroneously infer causal relationships where none exist.

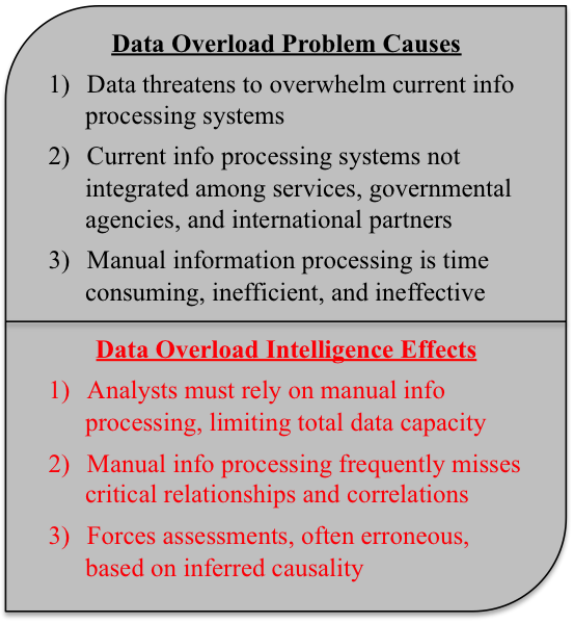


Figure 1: The Data Overload Problem

The first cause of the data overload problem is that the volume of data available to intelligence analysts is overwhelming. Current estimates of the amount of data available worldwide by 2020 range from 40 trillion gigabytes to one zettabyte (10^{21}).[4] Theoretically the explosion of data represents a treasure trove of valuable information that intelligence analysts

[4] Kevin G. Coleman, "Drowning in Data," *C4ISRNET*, 11 April 2016, http://www.c4isrnet.com/story/military-tech/blog/net-defense/2016/04/11/data-overload-internet-of-things/82905526/.

can use to identify threats to the homeland, find and identify military targets, and pinpoint the location of high-value individuals, to name just a few military uses for data-driven intelligence assessments. However, this enormous amount of data threatens to overwhelm current information processing systems. According to Mark Pomerleau of C4ISRNet: "The Department of Defense is grappling with an overwhelming preponderance of data, so much so that it can't process it all."[5] Consequently, valuable intelligence collection is going unanalyzed, putting the homeland and troops in combat in jeopardy.

The U.S. military has recognized the data overload problem and begun to embrace automated information processing tools in an attempt to solve the problem. Unfortunately, the military intelligence community's information processing software is not integrated across services, governmental organizations, and international partners, the second major cause of the data overload problem. Intelligence analysts often have difficulty reaching across multiple programs and databases to access pertinent data. U.S. Air Force (USAF) Colonel Jason Brown, Commander of the 480th Intelligence, Surveillance, and Reconnaissance (ISR) Wing, explained the problem: "Much of the [intelligence] community still operates in closed information environments; even with intelligence networks of the same classification level, most intelligence data exists, disparate and unconnected, in isolated databases, spreadsheets, and proprietary systems."[6] The current, stove-piped system forces analysts to search for applicable data instead of it being sent to them. Dr. Jon Kimminau, a USAF Analysis Mission Technical Advisor, described how this manual process could stifle cross-organization coordination, "while analysts can collaborate today, it is more often a 'pull' system where one asks those who are known to be

[5] Mark Pomerleau, "DoD Has More Intel Than it Can Process," *C4ISRNET*, 20 March 2017, http://www.c4isrnet.com/articles/dod-has-more-intel-than-it-can-process.
[6] Jason M. Brown, "The Data-Driven Transformation of Intelligence," *The National Interest*, 25 February 2017, http://nationalinterest.org/blog/the-buzz/the-data-driven-transformation-intelligence-19570.

working a problem, rather than a 'push' system where analysts may be automatically alerted to other similar work."[7] The inability to access all available data from multiple collection platforms and organizations hamstrings analysts, limiting their ability to find and analyze pertinent data, resulting in missed correlations and relationships.

The third major factor in the data overload problem is that manual information processing is inefficient, time consuming, and ultimately ineffective. Navigating through organizational and disciplinary firewalls and manually correlating and fusing data takes a significant amount of an intelligence professional's time. According to Peder Jungck, Chief Technology Officer for BAE Systems Intelligence and Security Sector: "Analysts spend 60 to 70 percent of the time trying to collect the data they need…trying to find the needle in the stack of needles that [they] didn't know about."[8] Analysts devote the majority of their time to culling useful information from search results and data outputs rather than analyzing trends and relationships and building assessments.

This data overload problem hurts the quality of intelligence assessments provided to military commanders, civilian decision-makers, and other recipients of intelligence products. Depart of Defense (DoD) Joint Publication 2-0, *Joint Intelligence*, explains the intelligence analysis process: "During analysis and production, intelligence is produced from the information gathered by the collection capabilities assigned or attached to the joint force and from the refinement and compilation of intelligence received from subordinate units and external organizations. All available processed information is integrated, evaluated, analyzed, and

[7] Jon A. Kimminau, "Five Examples of Big Data Analytics and the Future of ISR," *Joint Force Quarterly*, April 2015, 31.
[8] Jungck is quoted in: Dan Parsons, "Automation Key to Tackling Burdensome Big Data Problems," *National Defense*, March 2014, pp. 24.

interpreted."[9] Unfortunately, the steps in this process are currently not automated. Intelligence analysts must pull information from various databases, manually fuse and analyze the results, which is much more time intensive than automated information processing. The imbalance between time dedicated to manual research vice analysis causes the three analytic problems discussed in the introduction that plague intelligence professionals. First, analysts are only capable of examining a limited amount of the data available, and failure to use all the available data increases the likelihood of missing vital relationships and correlations. Second, the overwhelming volume of available data drives data sampling, which leads to a distorted perception of reality when an analyst attempts to extrapolate the meaning of the data points at a larger scale. Finally, this distortion of reality often leads to inferred and erroneous correlation.

These intelligence analysis problems are seen even in operating environments that are saturated with intelligence collection assets and sensors, and analysts who have been working together for years to solve intelligence problems. USAF Lieutenant Colonel Chandler Atwood, the Chief of the Commander's Action Group for the USAF Deputy Chief of Staff for ISR, explained these intelligence analysis problems continue to plague coalition operations in Afghanistan:

> Even today in Afghanistan where ISR forces have been redundantly layered for years, the creation of a timely, coherent picture gained from integrated, multi-source intelligence data is a rarity. For instance, U.S. and North Atlantic Treaty Organization forces in Afghanistan have suffered losses when they were surprised by an unexpected larger insurgent force not detected and relayed in time even when there were ever-present ISR assets operating in a permissible environment. This assertion still stands true today and portends an enduring DOD intelligence enterprise challenge of integrating disparate datasets into a clear picture for warfighters and their commanders across all types of battlespaces.[10]

[9] Department of Defense, "Joint Publication 2-0, *Joint Intelligence*," 22 October 2013, pp. I-16.
[10] Chandler P. Atwood, "Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis," *Joint Forces Quarterly*, vol. 77, 2nd Quarter, 2015, pp.25.

Even though analysts from multiple organizations are pooling their resources to provide multi-source and multi-discipline solutions, the inability to quickly develop an accurate operating picture has resulted in combat losses. The data overload problem is the root cause of these losses; though critical pieces of information are available to the intelligence analysts, they are unable to rapidly fuse and correlate the data manually, resulting in assessments based on incomplete or inaccurate data. However, automated information processing promises to mitigate the data overload problem and reduce its harmful effects on intelligence analysis.

Part II: Big Data and Automated Information Processing

Big data is an often-used buzz phrase that is largely misunderstood. Before progressing in our examination of the potential benefits of big data and automated information processing, it is critical to define the term "big data." Viktor Mayer-Schönberger, Professor of Internet Governance at Oxford University, and Kenneth Cukier, Contributor at the *Economist*, in their groundbreaking book on big data define the term simply, "[b]ig data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value."[11] Big data, at its core, is simply a term that describes the ability to access and use vast amounts of data in new or unintended ways, such as finding previously unobserved trends, relationships, and correlations.

A method of accessing and using big data is automated information processing, also known as "big data tools." Automated information processing allows analysts to quickly find, organize, and search through massive amounts of data now available. Using data in new or originally unintended ways can help to find correlations and patterns that may not be identifiable by looking at smaller datasets or by sampling available data, as well as eliminating uncertainty

[11] Viktor Mayer-Schönberger and Kenneth Cukier, "Big Data," Mariner Books: New York, NY, 2013, pp. 6.

associated with sampling. Taken together, these processing tools and the resulting, data-driven conclusions are often called "big data analytics." The DoD has begun investing heavily in big data tools. Unfortunately, according to USAF Lieutenant General Jack Shanahan, Director for Defense Intelligence (Warfighter Support), Office of the Under Secretary of Defense for Intelligence, procurement has focused on "one off projects and ideas," as opposed to a coherent and coordinated effort.[12] Consequently, DoD's automated information processing tools are built for specific organizations, collection assets or sensors, and are not designed to reach across organizations, collection platforms and intelligence disciplines. However, according to General Shanahan, DoD is investing more than $500 million in fiscal year 2017 to solving this problem and acquiring tools that will automatically access, fuse, and correlate data.[13] With the imminent deployment of automated information processing tools, intelligence analysts must be prepared to use these tools.

When examining big data and its importance, it is critical to understand the primary benefit is not in the automated information processing per se, but rather in the data itself. This maxim is especially true with regards to intelligence analysis. Though there are huge benefits in being able to quickly fuse and analyze data from a host of collection sources and storage databases, the most important benefit is found within the data itself. The ability to access all the data, or as near to all the data as possible, opens a world of analytic opportunity for intelligence analysts. Instead of sampling the available data, an analyst will be able to use all of it to manipulate and test hypotheses quickly, finding previously unseen or unsuspected correlations and relationships.

[12] Pomerleau, "DoD Has More Intel Than it Can Process," http://www.c4isrnet.com/articles/dod-has-more-intel-than-it-can-process.
[13] *Ibid.*

Big data is not only used to explain why something happened, but also to predict future events. In fact, Mayer-Schönberger and Cukier argue that big data is most effective when being used to predict future activity: "Big data is about predictions…about applying math to huge quantities of data to infer probabilities…The key is that these systems perform well because they are fed with lots of data on which to base their predictions."[14] Businesses around the world have been using big data to predict buying trends, target customers, tailor advertisements, and ultimately maximize profits. A fascinating case study in the use of big data to uncover unexpected trends and predict future sales comes from retail behemoth Wal-Mart. Wal-Mart collects a petabyte (10^{15}) of data from its customers every hour.[15] In 2004, while analyzing their sales data, the company noticed an anomaly: sales of strawberry pop-tarts spiked immediately prior to a hurricane in the projected impact area of the storm. Wal-Mart used this information to change its store layout in hurricane prone areas, moving strawberry pop-tarts to the front of the store next to other emergency supplies such as batteries and bottled water. The results were staggering; sales of the breakfast treat increased seven-fold immediately prior to a storm impact.[16] It is highly unlikely a sales analyst would ever have been able to manually find this anomaly, but the use of big data provided a major economic boon to the company. Such unexpected correlations and predictive evaluations can be applied to intelligence analysis as well.

Big data improves the efficiency of the intelligence analyst easier by making research much easier. Big data tools will eliminate some of the issues associated with searching through

[14] Mayer-Schönberger and Cukier, "Big Data," pp. 11-12.
[15] DeZyne.com, "How Big Data Analysis helped increase Walmarts Sales Turnover?" 23 May 2015, https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109.
[16] The pop-tart anecdote is from Mayer-Schönberger and Cukier, "Big Data," pp. 54. It was examined and expounded upon by the online business training company DeZyre. The data for the seven-fold increase in sales comes from a DeZyre article; "How Big Data Analysis helped increase Walmarts Sales Turnover?" 23 May 2015, https://www.dezyre.com/article/how-big-data-analysis-helped-increase-walmarts-sales-turnover/109.

multiple and often incompatible databases. Dr. Kimminau believes automated information tools will allow intelligence analysts to reach across service, organization, domain, and disciplinary walls to find, fuse, and correlate information for the intelligence analysts: "Big data analytics expand the avenues for collaboration and multidisciplinary, shared expertise in a global, distributed enterprise."[17] Big data tools thus can shift the balance of time intelligence analysts spend on research versus analysis, weighting their time to exploring, analyzing, and ultimately assessing the collected data. Big data and automated information processing are proliferating quickly; the question for intelligence analysts is how to use the data and tools to improve their tradecraft.

Part III: New Analytic Mindset – Follow the Correlation

Military intelligence is an essential component of warfighting and has existed as long as war. Master military theorist Carl von Clausewitz defines intelligence as the totality of available information on one's enemy, "[b]y 'intelligence' we mean every sort of information about the enemy and his country."[18] For centuries, military professionals have used every available collection method to determine the number, disposition, and intention of enemy forces. Now, as collection sensors, sources, and methods continue to increase in number and capability, the primary question posed to intelligence professionals will likely move from "how will I collect information on the target," to "which sets of information about my target are most useful?"

Modern military intelligence analysts are taught to work with available data to make an assessment on future enemy actions. They are also taught that they will be forced to work with incomplete data, and to make educated predictions based on the data available, their experience,

[17] Kimminau, "Five Examples of Big Data Analytics and the Future of ISR," 31.
[18] Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976), pp. 117

and knowledge of the target. However, this push for experience-driven assessments can exacerbate cognitive biases in the intelligence analysis and production process. According to Colonel Brown: "Intelligence is, for the most part, production focused, meaning many analysts are often forced to make quick assessments from limited text-based sources to meet deadlines. As such, they are trapped into making predictions that put too much weight on personal experience and cognitive bias."[19] Big data will allow the intelligence analyst to be led by data-driven conclusions vice experience-based assessments, which are rife with cognitive bias. Big data will not change the fundamental nature of intelligence, analysts will always have to use imperfect and incomplete information to make assessments, but it has the potential to change the character of intelligence analysis, from experience-driven to data-driven.

Increased data availability and the tools to find and analyze the data also have the potential to speed up the intelligence analysis process. As already discussed, the manual data search, correlation, and fusion process is time consuming. By reducing the time required for this phase of the intelligence cycle, assessments are made more rapidly, and commanders can make decisions more quickly. Ted Girard, Vice President of Delphix Federal, an Information Technology company that works with the US government describes the asymmetric advantage of using big data to quicken the pace of decision-making: "Future advantages afforded by big data are dependent on the ability to store, access and analyze unique data and deliver this information through different networks to the point of need, better and faster than our enemies. This is a big reason why data virtualization plays a critical role in producing actionable intelligence in a timely manner."[20] Girard's "data virtualization" refers to accessible data clearly presented to an

[19] Brown, "The Data-Driven Transformation of Intelligence," http://nationalinterest.org/blog/the-buzz/the-data-driven-transformation-intelligence-19570.
[20] Ted Girard, "How Defense Agencies can Better Cope with Big Data," *National Defense*, June 2015, pp. 21.

analyst, a key component of big data tools. Such virtualization is critical to providing timely and actionable intelligence more quickly than one's adversary.

Girard's analysis shows how big data can be leveraged to make decisions more quickly than one's enemy, a vital component of military strategist John Boyd's theory of conflict. Central to Boyd's theory is his Observe-Orient-Decide-Act (OODA) loop, which explains how individuals and organizations make decisions.[21] Intelligence collection is how one observes the adversary. Orientation, which Boyd described as the most important step in the loop,[22] is typically based on the intelligence assessment of the adversary. The use of data-driven correlations will provide a more complete picture and set of inputs to the "observe" stage of Boyd's loop, while data-driven assessments provide more accurate information to the "orient" stage of the loop. Royal Netherlands Lieutenant Colonel Frans Osinga, in his analysis of Boyd's work in general, and the OODA loop in particular, described the importance Boyd put on orientation of ingested information: "Observation is the task that detects events within an individual's, or group's environment. It is the method by which people identify change, or lack of change, in the world around them…Without the *context* of Orientation, most Observations would be *meaningless* (emphasis addes)."[23] Big data, automated information processing tools, and data-driven analysis enables not only quicker, but better decision-making than one's adversary.

[21] Boyd's OODA Loop is often misconstrued to mean that whoever has the quickest decision-making loop will win a conflict. However, according to Boyd, accuracy of inputs and understanding of the operating environment, as well as tempo of decision-making is as important as rapid decision-making. A more complete and rich understanding of the OODA Loop can be found in Frans Osinga's book, *"Science, Strategy and War: The Strategic Theory of John Boyd"* (New York: Routledge, 2007). See Appendix C: Boyd's OODA Loop for Boyd's graphical depiction of his OODA loop.

[22] John R. Boyd, *The Essence of Winning and Losing*, January 1995, slide 4. Boyd states "orientation shapes observation, shapes decision, shapes action."

[23] Frans Osinga, "Science, Strategy and War: The Strategic Theory of John Boyd," New York: Routledge, 2007, pp. 230.

Current and future warfare will be dependent on speed and tempo of decisions and operations, but quick decisions based on poor information is a recipe for military disaster. Instead, dominance of the information domain, or accurate "orientation," is critical to prevailing in future conflicts. Lieutenant General VeraLinn "Dash" Jamieson, the USAF Deputy Chief of Staff for ISR, explains how the use of fused data to enable information dominance is key to future conflicts, which she refers to as "fusion warfare:"[24]

> In future conflicts, the victor may not necessarily be the one with the quickest OODA Loop. Rather, the prevailing side may be the one which can harness the power of multiple OODA loops, utilize the *vast amounts of data* in them, and provide enhanced battlefield situational awareness—all fused into decision-making analysis—to achieve multi-domain freedom of action…The victor will be able to *observe* and *orient* himself in a conflict *more accurately* and *faster* than his opponent, thereby deciding and acting *more rapidly and precisely*…[A] true capability leap lies in the ability to fuse the information together in a time and space of our choosing to deliver *actionable intelligence* to decision-makers (emphasis added).[25]

The use of big data and automated information processing tools is critical to achieve General Jamieson's vision of fusion warfare. The use of data-driven assessments will deliver the actionable intelligence commanders need to rapidly and accurately orient to the operational environment, allowing them to make *better* decisions *faster* than the adversary.

In order to use big data effectively, an intelligence analyst must develop the understanding of big data and the opportunities it provides. Girard contends that effectively using big data requires a mindset shift among intelligence analysts: "Big data requires a new way of thinking and a new approach to data management and analysis in order to avoid getting buried

[24] The term "fusion warfare" was coined in 2015 by then-Major Amanda Figueroa. Then-Major General Jamieson embraced the term and it has since been integrated into common Air Combat Command and USAF parlance to describe the character of information-driven future conflicts. See U.S. Air Force Public Affairs, "Fusion Warfare Key to C2 Future," *Air Force Online*, 2 March 2017, http://www.af.mil/News/ArticleDisplay/tabid/223/Article/1100441/fusion-warfare-key-to-c2-future.aspx.

[25] Jamieson, Maj. Gen. VeraLinn and Lt. Col. Maurizio Calabrese. "An ISR Perspective on Fusion Warfare." *Mitchell Institute Forums*, No. 2 (December, 2015), pp. 3.

under the massive mounds of information that military organizations generate."[26] The use of big data and automated information processing creates the opportunity to transform intelligence analysis, but analysts must look at the data with a "big data mindset." Mayer-Schönberger and Cukier identify three components of the mindset shift required to harness big data. First, the ability to analyze huge amounts of data obviates the need for sampling small amounts of data and inferring results. Second, big data eases the burden of exactness and the need to count and examine only what we perceive as the most important items. When data is limited, analysts tend to strive for perfection of data inputs, ignoring outlying or confusing data that they perceive may throw off all the results. However, this discarded data could contain the critical piece(s) of information in finding a high-value individual (HVI) or a mobile missile. Finally, big data emphasizes data-driven correlation instead of inferred causation.[27] When the answer to an intelligence problem or question is not obvious, an analyst will tend to make an assessment or correlation based on experience, which Colonel Brown previously warned was a major factor in cognitive bias influencing intelligence assessments. These three shifts represent a transformation in the way intelligence analysts examine and assess an intelligence question.

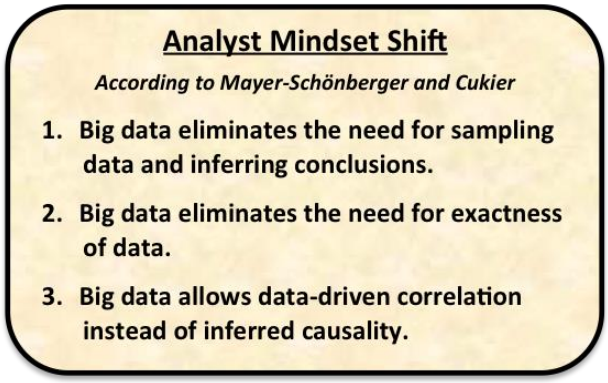


Figure 2: The Analytic Mindset Shift

The most important component of this mindset shift is overcoming the inherent bias towards inferred causality in favor of data-driven correlation. It is important to distinguish correlation as it is used in the intelligence process, and in the field of big data. Correlation in the

[26] Girard, "How Defense Agencies can Better Cope with Big Data," pp. 20-21.
[27] Mayer-Schönberger and Cukier, "Big Data," pp. 11-14.

intelligence process refers to a relationship between events or activities. For example, if an infrared sensor detected a missile launch, and a signals intelligence (SIGINT) sensor simultaneously collected an emission from a radar associated with the missile system, the two pieces of intelligence are likely from the same event and would be described as "correlated." However, correlation in the context of big data is based upon a statistical relationship between events as opposed to spatial or temporal correlation in the intelligence process. According to Mayer-Schönberger and Cukier, "[a]t its core, correlation quantifies the statistical relationship between two data values. A strong correlation means that when one of the data values changes, the other is highly likely to change as well."[28] When discussing big data and the correlation analytic mindset, the Mayer-Schönberger and Cukier definition is more applicable, and thus will be hereafter used when the term is used in the context of big data.

While correlation is based on data and a statistical relationship between events, causality is based on a conclusion of cause and effect. Humans have a fundamental bias in favor of causality because it is easier to understand cause and effect than probability. Mayer-Schönberger and Cukier explained this bias: "As humans we have been conditioned to look for causes, even though searching for causality is often difficult and may lead us down the wrong paths."[29] In the introduction we introduced the "post hoc, ergo propter hoc" cognitive bias (sometimes also called hindsight bias). This is perhaps the most prolific cognitive bias of inferred causality: Event B followed Event A; therefore A caused B. Unfortunately, without amplifying data this could very well be a faulty conclusion. Confirmation bias, or the tendency to interpret information in a

[28] *Ibid*, pp. 52-3.
[29] *Ibid*, pp. 14.

way that confirms one's preconceived notions is another frequently observed cognitive bias.[30] Reliance on experience-based inferred causality invites these types of cognitive biases into the intelligence analysis process.

The intelligence profession, by its very nature, manifests these biases. Commanders and decision-makers want to know not only that something is happening, but the reason why that thing is occurring. Intelligence analysts are unable to provide big data-driven correlation and must infer causality based on limited data because they do not have the tools to correlate, fuse, and analyze all of the data. The tendency is for analysts to use some of the data, or sample available data in the development of their assessments. Or worse, only use the data that supports the cause they want to promote, leaving out other data that may be relevant but does not support their conclusions. Mayer-Schönberger and Cukier continued their explanation of causation and correlation and why big data should be used to look for data-driven correlation: "In a big data world…we won't have to be fixated on causality; instead we can discover patterns and correlations in the data that offer us novel and invaluable insights. The correlations may not tell us precisely *why* something is happening, but they alert us *that* it is happening (author's italics)."[31] This shift from sampling and inferred causality to a correlation-focused analysis is the primary benefit intelligence professionals will reap from the use of automated information systems.

Analysis driven by correlation, especially unexpected correlation, can be controversial and contentious. This resistance was illustrated in an adverse reaction to a recently completed study at Yale University that attempted to identify data trends and/or relationships that may

[30] Johnny Jermias, "Cognitive Dissonance and Resistance to Change: The Influence of Commitment Confirmation and Feedback on Judgment Usefulness of Accounting Systems," *Accounting, Organizations & Society*. 26, 2, March 2001, pp. 146.
[31] Mayer-Schönberger and Cukier, "Big Data," pp. 14.

predict Afghan insurgent attacks. Kentaro Hirose of the Waseda University, Kosuke Imai, professor at Princeton University, and Jason Lyall, professor at Yale University, surveyed 204 villages in Afghanistan to determine local attitudes towards coalition operations. The research team plotted these villages, annotating their feelings towards the coalition, and then overlaid insurgent attack data and found a disturbing correlation. Positive feelings towards counterinsurgency operations correlated to increased insurgent attacks, and pro-coalition feelings did not correlate to an increase in the discovery of improvised explosive devices. Hirose, Imai, and Lyall summed up their findings:

> Three main findings emerge. First, we find that pro-counterinsurgent attitudes significantly improve the accuracy of predicting the location of insurgent direct attacks and the use of improvised explosive devices (IEDs) for up to 10 months after our survey…Second, we find little evidence that pro-counterinsurgent attitudes are associated with 'found' IEDs, suggesting that winning hearts and minds may not translate into actionable intelligence. Finally, these findings hold after adjusting for confounding variables such as prior insurgent violence, the location of ISAF and Afghan National Security Forces (ANSF) bases, and development aid.[32]

This correlation directly contravenes accepted counterinsurgency (COIN) theory, which holds that winning the hearts and minds of locals leads to an increase in security and a corresponding increase in thwarted insurgent attacks. According to the research team, their conclusions remain controversial and have not been widely accepted, and they are continuing to convince themselves and their peers that their conclusions, though unexpected, are valid.[33] The hostile reaction of military and civilian leaders should come as no surprise, as these conclusions have the possibility of fundamentally challenging the U.S.' current COIN theory.

[32] Kentaro Hirose, Kosuke Imai, Jason Lyall, "Can Civilian Attitudes Predict Insurgent Violence? Ideology and Insurgent Tactical Choice in Civil War." *Journal of Peace Research*. Vol. 54(1), 2017, pp. 48.
[33] Hossein Fatemi, "Modeling the Mob: How Computers can Predict Violence." *SciDev.Net*, 3 December 2015, http://www.scidev.net/global/conflict/feature/modelling-mob-computers-predict-violence.html

Hirose, Imai, and Lyall found this disturbing correlation by using large data sets instead of limited data samples. Naturally, they desired to explain the reason for the troubling trend. They explain their conclusion for the correlation between positive feelings towards coalition operations and insurgent attacks: "Efforts to win 'hearts and minds' may therefore have an unintended consequence: these efforts can attract increased insurgent attacks in areas where counterinsurgents have made the deepest inroads."[34] The analytic process the team engaged in is exactly the type of analysis that military intelligence professionals will use in a big data world. Analysts will need to access and cross-reference vast quantities of data, and they are likely to find correlations and relationships that they may not have expected.

The hostile reaction to Hirose, Imai, and Lyall's findings epitomizes the potential pitfalls of data-driven analysis that may plague military intelligence professionals and their commanders. This example is not designed to indict COIN theory; rather it is used to show that following correlation can lead to conclusions that may not be believed because they threaten widely held beliefs. The example provides valuable lessons for intelligence professionals and their commanders for producing and consuming big data-driven intelligence assessments. Intelligence analysts must look at the data-derived conclusions with an open mind, willing to accept unexpected correlations or unsuspected relationships. Commanders must be willing to accept that long-held beliefs about causality may be disproven by data-driven assessments.

[34] Hirose, Imai, and Lyall, "Can Civilian Attitudes Predict Insurgent Violence?" pp. 48.

Part IV: Using the Digital Data Trail

Section 1: *Tracking the Digital Data Trail in a Big Data World*

In order to leverage big data, intelligence analysts must learn to search for the digital data trail that all individuals and organizations leave. Mayer-Schönberger and Cukier explained this phenomena: "A term of art has emerged to describe the digital trail that people leave in their wake: 'data exhaust.' It refers to data that is shed as a byproduct of people's actions and movements in the world."[35] The data exhaust includes, but is not limited to, cell phone calls, social media posts, credit card purchases, and WiFi logins. This data trail is the key to intelligence professionals' use of big data and automated information processing. Each piece of data left in this data exhaust could lead military forces to a target, improve battlefield situational awareness, or be used in a host of other ways.

Colonel Brown believes that this data trail has altered how military intelligence professionals can find and report on adversary action. He explained that information not considered traditional intelligence collect such as social media activity can be a tip for finding and tracking an adversary: "That ability now involves seeing the data trails left by every actor engaged in conflict. This not only includes data ISR capabilities produce, but data anyone in proximity can produce. A simple tweet by a Pakistani IT consultant could have blown the cover of the SEAL team sent to kill Osama bin Laden. The lesson: if you're not already leaving a data trail, someone will create it for you."[36] A critical point that Colonel Brown makes is that others may leave a digital trail for you, as was the case in the Bin Laden raid. Military intelligence professionals need to understand how to search for these data trails, left both by the target and

[35] Mayer-Schönberger and Cukier, "Big Data," pp. 113.
[36] Col Jason M. Brown, "In the Information Age Centers of Activity > Centers of Gravity," *Medium*, 5 May 2015, https://medium.com/the-bridge/in-the-information-age-c70622a61bc9#.23fuplly2.

those in contact with, or close proximity to the target, and how to operationally use the data contained within the data exhaust. Big data allows this data trail to be combed, looking for previously unseen or unsuspected relationships and/or tendencies. Analysts can use data-driven conclusions to find, track, or predict future movements of military targets.

Finding an HVI is potentially the simplest example to describe how to operationally use a digital data trail. Any HVI that uses a cell phone or a social media account, or any other type of digital interaction or transaction will leave data in their digital exhaust. An intelligence professional might use that digital data trail to not only identify the last known location of the HVI, but also predict the future location of the individual and what type of digital trail they will create in the future. Colonel Brown explained how we can use a data trail to enable operations, "[w]e may not entirely know what the enemy is doing and why, but we know it's him and we know where we need to act."[37] Tracking HVIs is just one example of data-driven intelligence assessments enabling military operations. These data trails can also aid in a hunt for a military unit, such as a mobile reconnaissance unit, a surface-to-surface missile firing unit, or a SAM battalion. The same core competencies of understanding and using big data and automated information processing can be used to hunt HVIs or SAMs, or any other mobile target.

Section 2: *Finding a Mobile Surface-to-Air Missile System Case Study*

The hunt for a mobile threat, in this case study a modern, long-range SAM system like the Russian-produced S-400 (NATO Designator: SA-21 GROWLER), is an example of how an intelligence professional could use big data tools to find a target. Hunting SAMs is critical for the establishment of air superiority, usually a requirement for all U.S. military operations. This

[37]Brown, "In the Information Age Centers of Activity > Centers of Gravity," https://medium.com/the-bridge/in-the-information-age-c70622a61bc9#.23fuplly2.

particular SAM is incredibly dangerous to U.S. air operations as it is designed to be mobile; to kill aircraft at ranges exceeding 130 nautical miles, and to defend critical targets from missile and drone attacks.[38] Finding and killing this SAM is one of the most difficult problems facing coalition air planners, and thus is an intriguing and topical case study for the use of big data tools and data-driven, correlation-focused intelligence assessments in a major contingency operation.

When searching for mobile targets, military intelligence analysts study their target and search for detectable signatures associated with that target. A detectable signature is a specific piece of data that can provide an indication of the target's identification and location. The most identifiable detectable signatures of any SAM are the system's associated radars, which can be collected via SIGINT sensors that can identify and locate emissions from target radars. In the case of the S-400, there are three radars that emit detectable signatures associated with the SAM system; the BIG BIRD battle management radar, the CHEESEBOARD target acquisition radar and the GRAVE STONE target engagement radar. The BIG BIRD operates at the SAM Group (equivalent to Brigade level), and can control multiple S-400 battalions, also known as firing units.[39] As such, the BIG BIRD may not be co-located with any of the S-400 firing units. Therefore, the intelligence analyst must focus on collecting on and locating the battalion's primary radars, the CHEESEBOARD and GRAVESTONE, which are located with the firing units, and are the primary targets for strike. However, militaries throughout the world

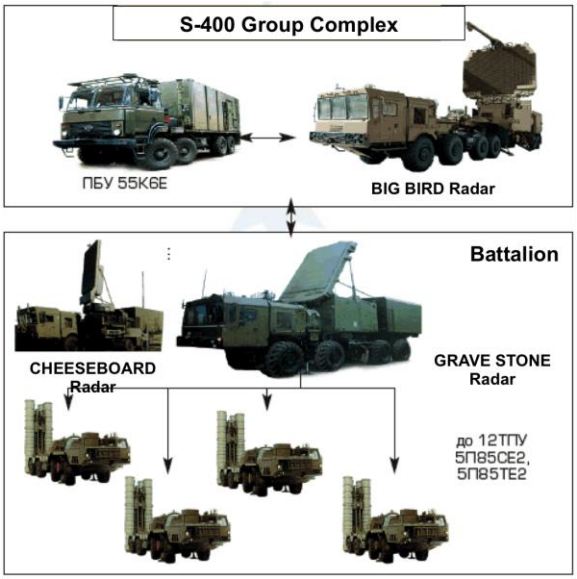


Figure 3: Components of the S-400 SAM
(graphic courtesy of AirPowerAustralia.net)

[38] Dr. Carlo Kopp, "Almaz-Antey 40R6 / S-400 Triumf, Self Propelled Air Defence System / SA-21," *Air Power Australia*, May 2009, http://www.ausairpower.net/APA-S-400-Triumf.html.
[39] Kopp, "Almaz-Antey 40R6 / S-400 Triumf," http://www.ausairpower.net/APA-S-400-Triumf.html.

are aware of the detectability of radar emissions and utilize emissions control and limit their radiation of these radars, leaving intelligence professionals looking for more discreet detectable signatures of the system.

Any voice or digital communication from any component of the system or its personnel can help intelligence professionals find the system. Datalinks, radios, cell phones, and personal social media posts all provide clues as to the location of the system. Assuming the intelligence community could collect some, or all of these devices and communications, there could be a wealth of data available to scour to find the SAM, or use data-driven analysis to predict future movement of the battalion. If intelligence professionals were forced to use a multitude of databases to manually search for these clues, fuse the data and extrapolate the most likely locations of the system, one could imagine how laborious this process would be and how unlikely to provide timely and actionable intelligence on the system's location.

The use of big data and automated information processing systems provides the potential to speed this process and provide a more complete and contexualized picture of the threat SAM's operations. Imagine the potential of software to cull this information near instantaneously to identify previously unseen relationships. Let us assume, as a hypothetical, that a 19-year old conscript is a missile loader in a particular S-400 battalion. As part of a quarterly mobility exercise the battalion is required to leave garrison and establish a new operating position in a covered position, say a wooded forest. When the battalion arrives at the new operating location, the Private radios his battalion chief that his missile loader has arrived, while the missile launcher sends a datalink update to its command post that it is in good working order. The Private then calls his girlfriend at home telling her he has made the trip safely and then posts a selfie of himself sitting on the missile launcher on Facebook, and includes the hashtag

#CampingWithS400. Each of these actions, a radio call, the datalink message, the cell phone call, and social media post has all provided clues as to the battalion's location.

Were there sensors that were capable of collecting each of these signatures, big data software could theoretically correlate certain cell phone numbers and datalink message types to this particular S-400 unit and provide a tip to an intelligence professional sitting at a Distributed Ground Station at Langley Air Force Base in Virginia. The Senior Airman who sees the message could request a U-2 image of the location and within the hour she could be examining a high-resolution image of a SAM battalion partially undercover in a forest. She could forward the image to a targeteer also at Langley, and within minutes the coordinates of the S-400 unit could be sent to an F-22 via datalink. In the course of two hours or less, the intelligence analyst could leverage big data tools to find the SAM, determine its location, generate global positioning system (GPS) coordinates for the site, and forward the intelligence to a tactical platform. Were this example set in wartime, the S-400 could be destroyed by the F-22 or another strike platform within minutes of receiving the GPS coordinates of the target. This is a preview of "fusion warfare" as envisioned by General Jamieson.

This scenario may not be as improbable as it may seem at first impression. In the immediate aftermath of the Malaysian Airlines MH17 crash, there was a question as to what brought the aircraft down. The speculation quickly centered on a missile, but the question became whether the missile was fired from a Ukrainian aircraft (as claimed by the Kremlin), a Russian military unit, or a Russian-backed opposition group. A group of online sleuths known as Bellingcat scoured social media posts to find evidence that could conclusively answer the question of how the aircraft was attacked. Bellingcat quickly honed in on a Russian-made BUK SAM (NATO Designator: SA-11 GADFLY) because of an Associated Press picture of a BUK

firing unit in the vicinity of the shoot down. Maxim Tucker of *Newsweek* published an article explaining how this group uncovered conclusive evidence of Russian culpability through social media activity;

> Using social media posts and YouTube videos like pieces of a jigsaw puzzle, [Bellingcat] have been able to fill in holes about what happened on various battlefields across the globe. These self-taught open-source intelligence analysts can geolocate a Facebook video of a missile launch by matching the landscape to a different image on Google Earth, or use Instagram posts to track armored vehicles as they trek across rugged terrain.[40]

Belingcat did not use sophisticated big data and automated information processing tools, but rather searched social media sites manually to find pieces of evidence. Their example shows the potential of using a data trail to identify military activity. Were they military intelligence analysts with access to a multitude of classified and unclassified data sources, and automated information processing systems to near-instantaneously collect, fuse, and correlate data correlated to BUK activity, they may have been able to come to their conclusions much more quickly. The point of this example is not to show the benefit of exploitation of social media, but rather how non-traditional forms of intelligence, in the form of the digital data trail, can be used to find an advanced military threat like a SAM battalion.

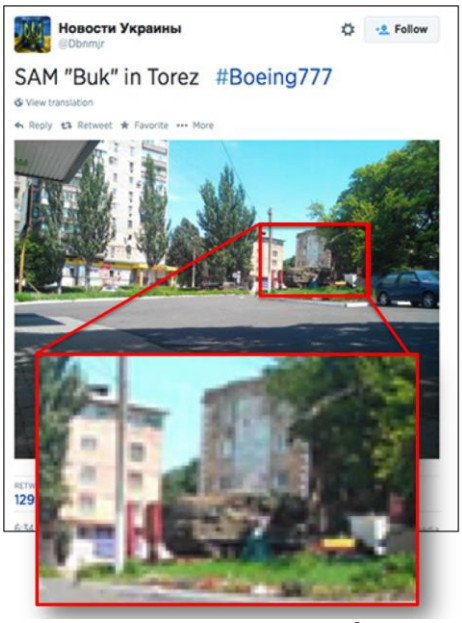


Figure 4: Twitter post confirming BUK firing battery near the site of the MH17 shoot down

[40] Maxim Tucker, "Meet Eliot Higgins, Putin's MH17 Nemesis, *Newsweek*, 22 June 2015, http://www.newsweek.com/2015/07/03/meet-eliot-higgins-putins-mh17-nemesis-345485.html.

Part V: Conclusion – Using Big Data and Automated Information Processing

Military commanders and civilian decision-makers rely on timely and actionable intelligence assessments as the basis for most, if not all of their decisions. Intelligence professionals are skilled in their use of available information, contextual knowledge, and experience to fill in the blanks and make intelligence assessments. Big data and automated intelligence processing provides the opportunity for intelligence analysts to use exponentially more data to find unexpected correlations and identify unsuspected relationships which can be used as the basis for data-driven intelligence assessments. Dr. Kimminau explained the potential offered by big data and automated information processing: "Big data analytics offers the potential to revolutionize how analysis supports our warfighters and national decision-makers with intelligence—the decision advantage in national security."[41] Big data tools make Kimminau's "decision advantage" a reality. The ability to quickly access, fuse, correlate, and manage vast amounts of data can fundamentally transform the intelligence analysis process.

Big data and the ability to leverage its awesome capability through automated information processing offers intelligence analysts a unique opportunity to vastly improve not only the timeliness and accuracy of intelligence assessments, but also to improve their ability to predict future events. The intelligence community is just beginning to discuss and debate the use of big data tools to fight "near-peer conflicts." It seems clear that intelligence personnel and agencies will attempt to leverage big data to fight future conflicts. What is not clear at this time is how analysts need to adapt and be trained to be ready to use big data and automated information processing tools. In order to harness the power of big data, intelligence professionals must move from current thinking that focuses on data sampling and inferred causality, and instead focus on a data-driven, correlation-focused analytic process. This fundamental shift in

[41] Kimminau, "Five Examples of Big Data Analytics and the Future of ISR,".

intelligence analysis will allow military intelligence professionals to explain what is, if not why it is, and provide more predictive assessments on enemy activities and locations.

We live in a world of digital data, and big data is simply a term that describes a method of accessing and working with massive amounts of data. Commercial industries have embraced the big data revolution, and it is clear the U.S. military sees that big data provides huge potential benefits. Military intelligence may be the combat capability that benefits most from big data and automated information processing. These tools are quickly gaining a foothold in the US military, but intelligence analysts are not being taught how to use big data. Intelligence professionals must learn to embrace data-driven analysis that combines observed adversary activity, correlations and relationships that may not have been expected or even run counter to conventional wisdom. Following data-driven analysis that weighs correlation over inferred causality is a critical first step in understanding how to effectively utilize big data. Military commanders and governmental decision-makers also have a responsibility in fostering the big data revolution within the military. They must be aware of the changing face of intelligence analysis, and be prepared to accept a data-driven correlation that may be unable to answer the why, or causation. Mastering the use of big data may give the U.S. a generational advantage over their adversaries in providing more complete, timely, and accurate inputs that inform and quicken the tempo of our OODA Loop, and provide our military forces an asymmetric advantage on the battlefield.

Appendix A: *Joint Military Definitions and Terms*

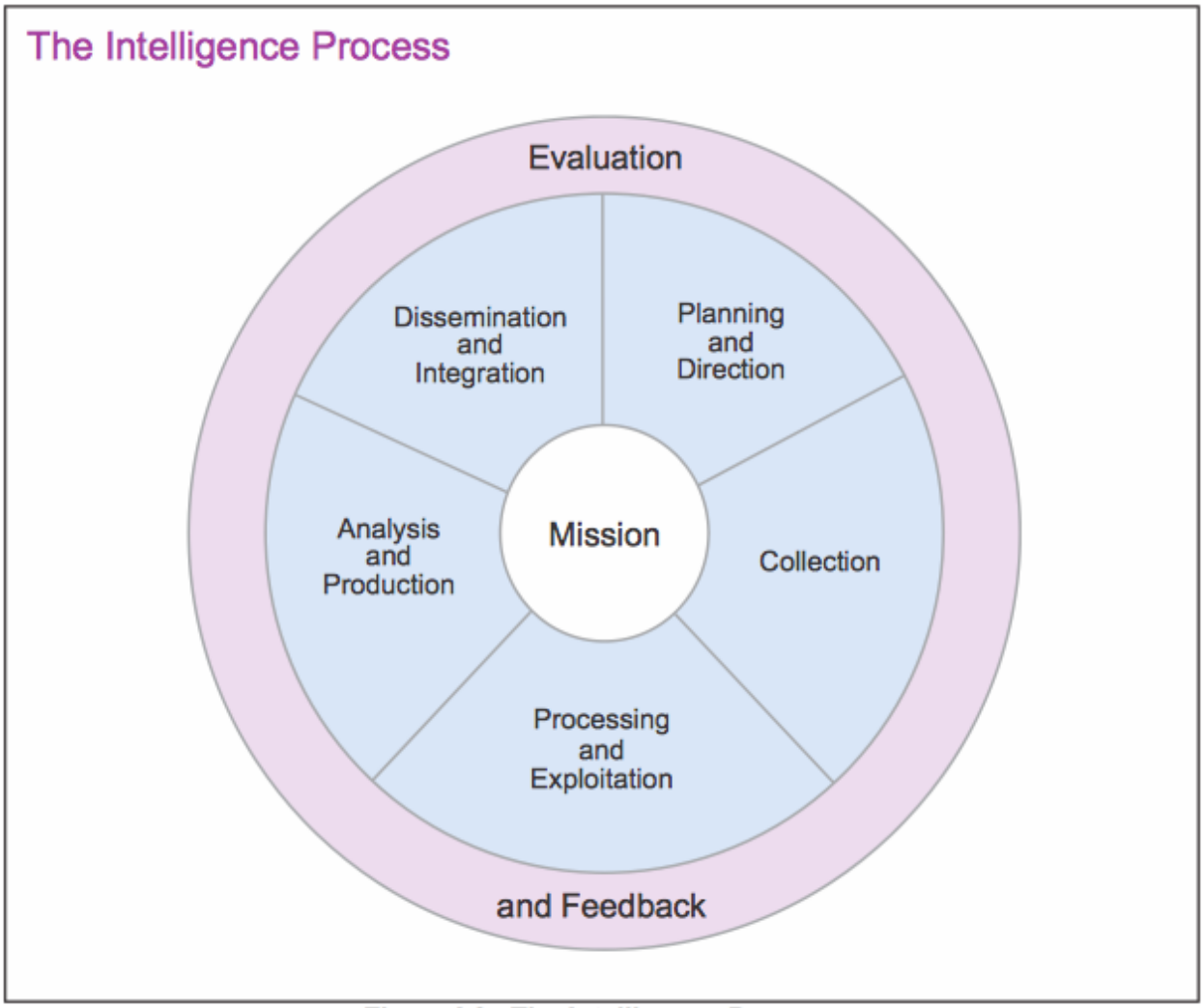
Analysis and Production: intelligence is produced from the information gathered by the collection capabilities assigned or attached to the joint force and from the refinement and compilation of intelligence received from subordinate units and external organizations (JP 2-0, pp. I-16).

Correlation: (not defined in joint doctrine) the relationship between things that happen or change together. (www.merriam-webster.com/dictionary/correlation)

Fusion: a deliberate and consistent process of collecting and examining information from all available sources and intelligence disciplines to derive as complete an assessment as possible of detected activity (JP 2-0, pp. II-12).

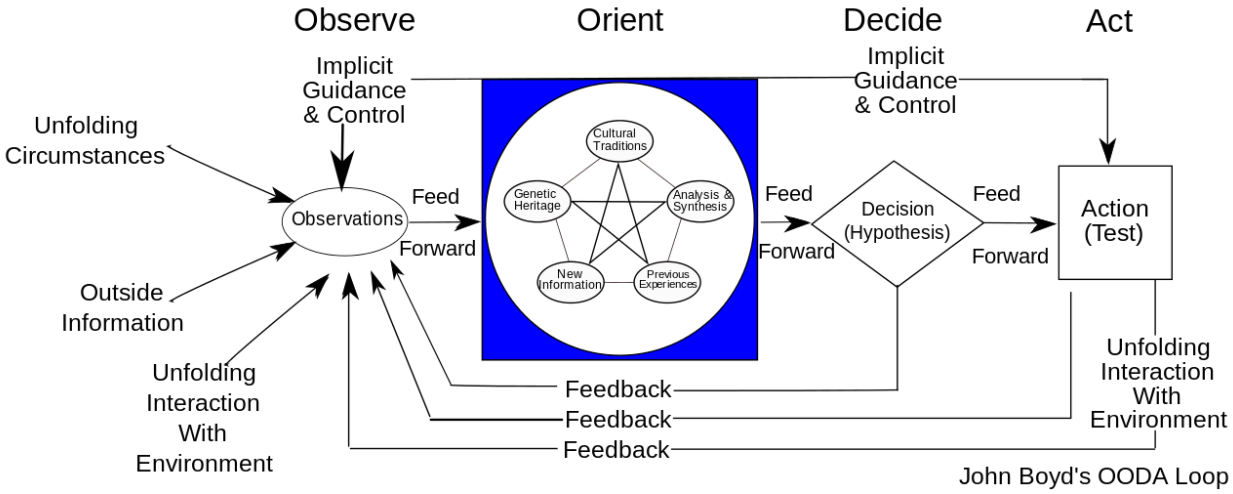
Intelligence Assessments: predictive, accurate, and relevant intelligence estimates (JP 2-0, pp. I-1).

Appendix B: *The Intelligence Process*



Joint Publication 2-0, *Joint Intelligence* (22 Oct 2013), pp. I-6

Appendix C: *John Boyd's Observe – Orient – Decide – Action (OODA) Loop*



Glossary

ANSF: Afghan National Security Force

COIN: Counter-Insurgency

DoD: Department of Defense

GPS: Global Positioning System

HVI: High-Value Individual

IED: Improvised Explosive Device

ISAF: International Security Assistance Force

ISR: Intelligence, Surveillance, and Reconnaissance

JP: Joint Publication

NATO: North Atlantic Treaty Organization

OODA: Observe – Orient – Decide - Act

SAM: Surface-to-Air Missile

SIGINT: Signals Intelligence

USAF: United States Air Force

Bibliography

Atwood, Lt. Col. Chandler. “Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis.” *Joint Forces Quarterly*, vol 77, April 2015: 24-33.

Boyd, John R. *The Essence of Winning and Losing*, January 1995 (presentation, 5 slides).

Brooks, Nichoel E. and Jami Forbes. 2015. "Enabling Decision Confidence by Mitigating Four Interacting Dilemmas Facing the Army Intelligence Enterprise." *Military Intelligence Professional Bulletin* 41 (2): 40-43.

Brown, Col. Jason M. “In the Information Age Centers of Activity > Centers of Gravity.” *Medium*, May 5, 2015, https://medium.com/the-bridge/in-the-information-age-c70622a61bc9#.23fuplly2.

----------. “The Data-Driven Transformation of Intelligence.” *The National Interest*, 25 February 2017, http://nationalinterest.org/blog/the-buzz/the-data-driven-transformation-intelligence-19570.

C4ISRNET. “Big Data Takes a Strategic Turn at DoD.” *C4ISRNET News*, 20 November 2014, http://www.c4isrnet.com/story/military-tech/it/2014/11/19/big-data-takes-a-strategic-turn-at-dod/19325227/.

Clausewitz, Carl von. On War, edited and translated by Michael Howard and Peter Paret (Princeton, New Jersey: Princeton University Press, 1976)

Coleman, Kevin G. “Drowning in Data. *C4ISRNET*, 11 April 2016, http://www.c4isrnet.com/story/military-tech/blog/net-defense/2016/04/11/data-overload-internet-of-things/82905526/.

Department of Defense. “Joint Publication 2-0, *Joint Intelligence*.” 22 October 2013.

Fatemi, Hossein. “Modeling the Mob: How Computers can Predict Violence.” *SciDev.Net*, 3 December 2015, http://www.scidev.net/global/conflict/feature/modelling-mob-computers-predict-violence.html.

Girard, Ted. "How Defense Agencies can Better Cope with Big Data." *National Defense*, June 2015, 99 (739): 20-21.

Hirose, Kentaro, Kosuke Imai Lyall, Jason. “Can Civilian Attitudes Predict Insurgent Violence? Ideology and Insurgent Tactical Choice in Civil War.” *Journal of Peace Research*, Vol. 54(1), 2017, pp. 47-63.

Jamieson, Maj. Gen. VeraLinn and Lt. Col. Maurizio Calabrese. “An ISR Perspective on Fusion Warfare.” *Mitchell Institute Forums*, No. 2 (December, 2015).

Jermias, Johnny. “Cognitive Dissonance and Resistance to Change: The Influence of Commitment Confirmation and Feedback on Judgment Usefulness of Accounting Systems. *Accounting, Organizations & Society*. 26, 2, 141-160, March 2001.

Kimminau, Jon A. “Five Examples of Big Data Analytics and the Future of ISR,” *Joint Forces Quarterly*, vol 77, April 2015.

Kopp, Carlo. “Almaz-Antey 40R6 / S-400 Triumf, Self Propelled Air Defence System / SA-21.” *Air Power Australia*, May 2009, http://www.ausairpower.net/APA-S-400-Triumf.html.

Magnuson, Stew. 2013. "Defense, Intel Communities Wrestle with the Promise and Problems of 'Big Data'." *National Defense* 97 (712): 34-36.

Mayer-Schönberger, Viktor, and Kenneth Cukier. “Big Data” Mariner Books: New York, NY, 2013.

Minear, Maj. John M. “Chasing Relevance: Building Actionable Intelligence Analysis.” *Mitchell Institute Forums*, No. 5 (June, 2016).

Osinga, Frans P.B. “Science, Strategy and War: The Strategic Theory of John Boyd” (New York: Routledge, 2007).

Parsons, Dan. "Automation Key to Tackling Burdensome Big Data Problems." *National Defense* 98 (724): 24-25.

Pomerleau, Mark. “DoD Has More Intel Than it Can Process.” *C4ISRNET*, 20 March 2017, http://www.c4isrnet.com/story/military-tech/data/2015/02/27/dod-intell-community-zero-in-on-big-data-analytics/24137255/.

Tadjdeh, Yasmin. 2015. "Big Data Analytics Helping to Secure the Seas." *National Defense* 100 (741): 19.

Tucker, Maxim. “Meet Eliot Higgins, Putin’s MH17 Nemesis. *Newsweek*, 22 June 2015, http://www.newsweek.com/2015/07/03/meet-eliot-higgins-putins-mh17-nemesis-345485.html.