MQ-9 Reaper remotely piloted aircraft at Holloman Air Force Base, New Mexico, December 16, 2016 (U.S. Air Force/J.M. Eddins, Jr.)

Open Sources for the Information Age

Or How I Learned to Stop Worrying and Love Unclassified Data

By James M. Davitch

After years of major spending on intelligence, surveillance, and reconnaissance (ISR) collection capabilities, the Intelligence Community (IC) is beginning to make a commensurate investment in technology to improve intelligence analysis.[1] However, absent a change that recognizes the increasing value of open source information, the IC will not realize a return on its investments.

This article investigates the origins of the modern IC and its tendency to rely on classified data to the exclusion of publicly available information, the utility of open source information and a new way of thinking about it as the key component for future early indications and warning (I&W), and a recommended way forward for the IC and possible steps for implementation of an open source information–enabled military intelligence force.

Harnessing the analytic potential in open source data, rather than closely guarded secret information, is *the* Big Data challenge facing intelligence professionals. Open source information may be the first indication of an adversary's hostile intent in what Department of Defense (DOD) leaders call the likely future threat environment.[2] But the IC bureaucracy remains locked in habitual patterns focused narrowly on classified

Lieutenant Colonel James M. Davitch, USAF, is the Intelligence Operations Division Chief at Air Force Global Strike Command, Barksdale Air Force Base, Louisiana.

sources. The first step to understanding why requires observation of the IC's organizational culture.

A Culture of Secrets

The combination of the Pearl Harbor surprise attack and a decentralized intelligence apparatus divided between the U.S. Army and Navy led many to believe the United States was vulnerable to another unforeseen strike. This led President Harry Truman to consolidate the intelligence mission, which, he hoped, would identify preliminary I&W of foreign aggression. Thus the 1947 creation of the Central Intelligence Agency (CIA) was, in essence, a hedge against future surprises.[3] So began the period of Industrial Age intelligence running from 1947 to about 1990.

The IC's narrow focus on the development and capabilities of the Soviet Union made "national intelligence" the primary feature of collection and reporting. The Soviet Union represented a complicated target and information about it was sparse. But as an intelligence problem it was "comparatively less complex" to today's globalized, interconnected, and interdependent geopolitical setting.[4] The Soviet Union's closed society and impressive counterintelligence architecture made necessary the development of expensive sensors and platforms to provide highly sought after puzzle pieces in this denied environment.[5] In the words of Gregory Treverton, "In the circumstances of the high Cold War, there were powerful arguments for targeting intelligence tightly on the Soviet Union, for giving pride of place to secrets, especially those collected by satellites and other technical means."[6]

The primary customer for Cold War intelligence was the President and National Security Council because it was the President who would bear the brunt of the blame if the United States suffered another surprise attack. Sensors and platforms were tailor-made to focus on counting Soviet aircraft, ships, and other military equipment. When the IC looked to open sources, it observed mostly the official messages and propaganda sent from the Soviet high command to the masses; this, it was presumed, might provide insight for the President into the adversary leadership's thinking.[7] However, the IC's weight of effort for planning and budgeting was geared toward exquisite collection systems.

The IC's focus on classified sources owes largely to the way it responds to the collection priorities laid out in the National Intelligence Priorities Framework (NIPF). The NIPF's purpose is to provide senior policy officials a vehicle to dictate a prioritized list of "critical interest" issues to the IC.[8] But the IC's toolkit is filled mostly with instruments that produce classified data. Therefore, it attempts to address NIPF priorities with the resources at hand and the methodologies deemed "proven" by victory in the Cold War. This perpetuates the acquisition and development of new sensors and platforms for the production of more classified information. The IC's method of responding to intelligence problems by looking predominantly to classified sources merits review.[9]

Breaking the current paradigm is difficult, but essential, if the IC is to assume a more proactive posture. Barriers to this goal include organizational inertia, the fear of untested alternative methods, and the satisfaction of answering simpler questions, no matter how illusory their utility. Large organizations seldom respond to change until after a crisis and instead follow established routines and simple standard operating procedures.[10] Under the prevailing intelligence collection construct, professionals perpetuate organizational inertia by engaging only in what Ronald Garst defines as *descriptive analysis*.[11] For example, analytical cells routinely provide statements describing what happened, when, and where, thereby eschewing predictive analysis.[12] Not coincidentally, U.S. intelligence sensors excel at providing data that supports descriptive intelligence analysis. But to this end, the IC is reactionary and fails to address what decisionmakers are often more interested in: describing what *will happen* and why. Daniel Kahneman refers to this tendency as the "substitution heuristic" whereby one simplifies difficult tasks by evaluating a related, easier question.[13]

The reliance on secret data derived from classified sources lends itself to answering intelligence questions quantitatively, such as the number of missions tasked and images collected and processed. These data are easy to numerically collect and aggregate, but it distracts from investigating qualitative indicators that might determine whether the intelligence process is contributing meaningfully to solving the underlying intelligence problem.[14] So the question, "Is our collection posture working to learn more about the enemy?" becomes instead, "How many ISR sorties have we flown in support of the leadership's priorities?"

It is important to note that while open sources may provide great utility, they are not a panacea for all intelligence problems. Each situation requires the requisite examination of its underlying characteristics. But the failure to address open sources' potential merits by reflexively dismissing it is, at best, a failure to consider creative solutions. At worst, it signals that the IC is unprepared to tackle the emergent complexity of global geopolitical dynamics and risks missing important I&W of future conflict.[15]

The 9/11 attacks provided the impetus for moving open source information into the forefront of the value proposition in that its ability to significantly augment traditional forms of intelligence rapidly became apparent in the counterterrorism mission. However, it was not until the advent of open source Big Data's velocity, variety, and volume characteristics, which became apparent with the explosion of social media, that the potential for greater open source analysis in lieu of an excessive focus on classified sources became a realistic possibility. One now might consider using open sources as the entry point for the intelligence collection process and using classified data to augment the unclassified source, thus flipping the paradigm upside down.

Flaws in the Technical Solution—It's Not *Only* About Secrets

Speaking to the Council on Foreign Relations, former CIA director Michael

Hayden described intelligence trade as a jigsaw puzzle.[16] The metaphor leads one to believe that all the pieces are available awaiting assembly. Unfortunately, this thinking typically translates to a need for more collection sensors that, in turn, promotes the exclusivity of classified information. All of this perpetuates the dubious contention that classified collection provides a window to truth. Moreover, it rewards both the pursuit and creation of more data, which burden analytical efforts. The net result is that the exclusivity of secret intelligence becomes the basis for analysis to the limitation, or even exclusion of, creative thinking.[17]

Intelligence problems, especially as they pertain to vague indications of impending hostilities, more resemble mysteries than puzzles. Anthony Olcott notes mysteries are difficult, if not impossible, to solve definitively, "no matter how much information is gathered," classified or otherwise.[18] Trying to answer mysteries usually involves uncertainty, doubt, and cognitive dissonance, which most seek to avoid. But embracing doubt and addressing probabilities are essential because so few intelligence problems lend themselves to easy, certain, factual answers. The only certainty with respect to intelligence mysteries is persistent uncertainty, which cannot be alleviated by simply throwing more surveillance sensors at the problem.

Philip Tetlock described the allure of certainty, stating that it "satisfies the brain's desire for order because it yields tidy explanations with no loose ends."[19] But Kahneman warns against the overconfidence certainty can provide: "Declarations of high confidence mainly tell you that an individual has constructed a coherent story in his mind, not necessarily that the story is true."[20] Doubt can sometimes be mitigated, though not eliminated, with more evidence that might even come from classified sources. But pointing to evidence exclusively derived from restricted data while claiming to have found truth is like a blind man describing the colors of a rainbow.[21]

While puzzles requiring the acquisition of secret "pieces" do persist, leveraging open source information is increasingly able to help us better understand mysteries *and* answer specific, defined problems. Open sources can point to breakthroughs in a nation's weapons research and development timeline, a task formerly the exclusive province of espionage or technical sensors. Asking questions like "What are the range and speed capabilities of the latest generation Chinese surface-to-air missile?" can be addressed through the lens of open sources.[22] Olcott illustrates the commercial, public-sector use of open sources, relating what Leonard Fuld calls the cardinal rule of intelligence: "Wherever money is exchanged, so is information."[23]

Considering the likely eventuality that intelligence problems of the future will more resemble mysteries than secrets, analysts will need to employ more creative and critical thinking and use a more diverse assortment of information than before. This will entail a greater mental workload for analysts used to the collect-process-analyze model traditionally centered on the classified collection. The IC's knee-jerk inclination to accept the answer offered by classified data satisfies what Daniel Kahneman calls our System 1 response, a mode of thinking in which the mind operates "automatically and quickly, with little or no effort."[24] Kahneman contrasts this mode with the concentration required of System 2, which "allocates attention to the effortful mental activities that demand it."[25] The uncertainty created by nebulous mysteries that often do not lend themselves to prompt answers, and the creative thinking required to solve them, is System 2 territory.

The IC's emphasis on classified information may ultimately be a barrier to creative thinking. Access to classified information carries with it the currency of prestige and the "need to know" restriction, which "fosters compartmentalized—reductionist—views of the issues at hand."[26] Josh Kerbel points to the Cold War era "when [the IC] had a relative monopoly on good information," which "continues to cause analysts to confuse exclusivity of information with relevance to decisionmakers."[27] During the Cold War, prized information was often technical and ephemeral, mainly consisting of communications and electrical emissions. Intelligence professionals often refer to this data as a "detectable signature" of the collection target. Such detectable signatures, fleeting during the Cold War, have exploded in the Information Age.

Wearable technology and the Internet of Things provide precise geolocation of an individual and connects one's previously private details to the open architecture of the Internet. Moreover, this information does not have to be secretly seized by a high-altitude sensor or through clandestine espionage. In fact, individuals *willingly* make their data available for observation. As Treverton noted, in the Information Age, "collecting information is less of a problem, and verifying it is more of one."[28] The open source environment provides detectable signatures of the adversary undreamed of prior to the advent of the Information Age.

The influx of open source data, including rapidly growing social media platforms, will only become more vital sources of information in the future. Kerbel notes, "[The IC] must get over its now illusory belief that its value-added comes mostly from information to which it alone has access—secrets."[29] Several open source social media companies are billion-dollar-a-year companies, to wit: Instagram. Founded in 2010, it is arguably the fastest growing social media channel, reaching 300 million users in 2016.[30] Alec Ross noted, "Today there are roughly 16 billion Internet connected devices. Four years from now that number will grow to 40 billion Internet-connected devices."[31]

Despite these publicly available sources of information, open source intelligence remains a lesser form of intelligence in the realm of intelligence disciplines. Treverton counters, "Intelligence now has . . . vast amounts of information . . . not a scarcity of information that mainly comes from satellites or spies and is therefore regarded as accurate."[32] Publicly available information is not only a valuable supplement, but it is also redefining I&W and should be used as the basis of future intelligence analysis. In essence, open sources should not augment secret

Soldiers with 82nd Airborne Division, Fort Bragg, North Carolina, and Italian Folgore Airborne Brigade, Vicenza, Italy, conduct Joint Forcible Entry Operation during Network Integration Evaluation 16.1, September 27, 2015, at White Sands Space Harbor, New Mexico (U.S. Army/Aura E. Sklenicka)

information, but the reverse. Doing so may pay dividends toward gaining essential warning in the nebulous current and future operating environments.

I&W—The Open Source Opportunity in "Hybrid War"

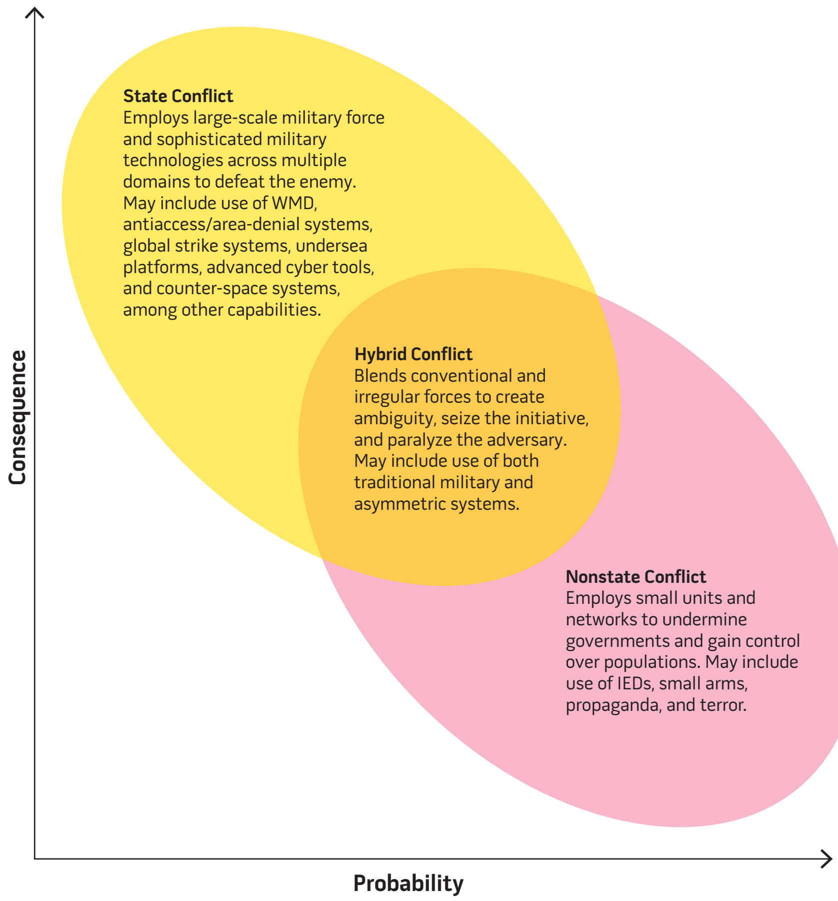
In the summer of 2014, "pro-Russian separatists" began appearing in eastern Ukraine. Moscow repeatedly denied that its regular forces were operating on Ukrainian soil, but social media truth gave lie to the Russian government's insistence. Young soldiers posted "selfies" to Instagram that, presumably unbeknownst to them, contained metadata that geolocated their position within Ukraine's borders. They provided strong evidence of Russia's complicity in the shootdown of Malaysia Airlines Flight 17.[33] Initial accounts rapidly flowed in from open sources to include pictures uploaded to Twitter and Instagram as well as numerous YouTube videos.[34] This type of cueing indication in and of itself does not constitute an "end product," but it could be used to direct traditional ISR collection assets to verify the open source tip.

Despite the crushing weight of evidence to the contrary, Russian defense outlets improbably assigned blame to Ukrainian forces.[35] Russian President Vladimir Putin, seizing the opportunity to win the propaganda war, crisply stated as much, declaring the situation could have been avoided "if Kiev had not resumed its military campaign against pro-Russian separatists."[36] These types of conventional and unconventional incidents mixed with intense public relations campaigns will be the U.S. military's most likely, and most dangerous, scenarios for conflict into the future.

General Martin Dempsey, former Chairman of the Joint Chiefs of Staff, offered (also outlined in the 2015 National Military Strategy, see figure) an appropriate definition of this type of information operation: "State and non-state actors working together toward shared objectives, employing a wide range of weapons such as we have witnessed in eastern Ukraine."[37] He continues, "Hybrid conflicts serve to increase ambiguity, complicate decision-making, and slow the coordination of effective responses. Due to these advantages to the aggressor, it is likely that this form of conflict will persist well into the future."[38]

Some have argued the concept of hybrid war in Ukraine is simply a continuation of conventional techniques and procedures.[39] Whatever the definition, what we are seeing is the most likely scenario for future conflict because it allows the adversary to do as Sun Tzu recommended: capitalize on the adversary's weaknesses while maximizing its own strengths. The U.S. military possesses overwhelming conventional might. But by engaging in disinformation and employing non-official military forces, the adversary can keep the conflict below the threshold where the United States might use its conventional advantage. As some have noted, such hybrid war strategies could "cripple a state before that state even realizes the

Figure. Continuum of Conflict


State Conflict
Employs large-scale military force and sophisticated military technologies across multiple domains to defeat the enemy. May include use of WMD, antiaccess/area-denial systems, global strike systems, undersea platforms, advanced cyber tools, and counter-space systems, among other capabilities.
Hybrid Conflict
Blends conventional and irregular forces to create ambiguity, seize the initiative, and paralyze the adversary. May include use of both traditional military and asymmetric systems.
Nonstate Conflict
Employs small units and networks to undermine governments and gain control over populations. May include use of IEDs, small arms, propaganda, and terror.
Consequence
Probability

conflict had begun," and yet it manages to "slip under NATO's [North Atlantic Treaty Organization's] threshold of perception and reaction."

This type of future conflict will not only be confined to the U.S. adversary in Eurasia. Michael Pillsbury describes China's possible employment of a military doctrine called "unrestricted warfare,"[40] which in many ways is analogous to these information operations.[41] One possible dangerous course of action in this region might entail the use of "civilian" Chinese fishing boats executing what for all intents and purposes is a military operation to solidify its assertion of territoriality. Such activities are not without precedent. Small-scale "fishing incidents" may become the source of increasing naval tensions. They provide China plausible deniability while remaining under the threshold for spurring greater U.S. military involvement.

As Steven Pifer noted in 2015 testimony before the U.S. Senate, irregular forces presaging larger conventional movements may be the example of future encounters.[42] General Philip Breedlove, the former U.S. European Command commander, also articulated these concerns, insisting NATO must be prepared to respond to "special forces without sovereign insignia who cross borders to create unrest" and ultimately destabilize countries.[43] However, traditional I&W techniques and ISR systems employed by the IC have historically focused on the deployment of large armed forces. They do so at the risk of missing earlier indications that might forestall conflict.

The Office of the Secretary of Defense's intention in pursuing the Third Offset concept is to deter potential adversaries from action. To that end, the IC's goal should be providing the timeliest I&W of impending conflict to avoid decision paralysis as the United States confronts entities falsely claiming noncombatant status. A sub-goal should be to provide decisionmakers with evidence to counter aggressor propaganda. The best tool for these missions in the future will likely not be a traditional collection platform originally designed to count Soviet tanks; it will be open source–derived information. Cold War–era tactics, techniques, and procedures are not conducive to identifying "little green men," innocuous fishing vessels, or the funding, arms, and leadership supporting them. Therefore, changing the way the IC conducts operations is warranted. That begins with a focus on open source information augmented by secret-seeking sensors capable of adding detail resulting in open source intelligence.

As the Third Offset implies, there is an important role for human-machine collaboration in this new open source–focused environment, specifically regarding artificial intelligence. While social media outlets like Facebook, Instagram, and Twitter are popularly used worldwide, some countries use other social media outlets more predominantly. The social networking sites VKontakte and QZone are the most popular outlets in Russia and China, respectively. Analysts must be cognizant of that fact and adept at deciphering not only foreign languages but also cultural nuances of the society in question. Automatic machine translation tools are rapidly improving and can help with both. In May 2014, Microsoft presented a computer program capable of translating spoken words in real time.[44] Describing the application of "deep learning" to machine translation, Maryam Najafabadi et al. relate how Google's "word2vec" tool can quickly learn complex relationships between hundreds of millions of words.[45] Using what are called "word vectors" allows the machine translator to distinguish nuance and context rather than literal translation. Artificial intelligence translation tools directed at social media outlets could provide a wealth of insight into lower level authority structures. Machine augmentation will not only allow us to hear what these individuals are saying, but also understand what they mean.

As part of USS *Sampson* Oceania Maritime Security Initiative mission, U.S. Navy Sailors and U.S. Coast Guard Pacific Law Enforcement Detachment Team personnel approach Chinese fishing vessel, November 29, 2016 (U.S. Navy/Bryan Jackson)

Recommendations

Major changes are required in the way military intelligence professionals think about problems. A cultural mindset change is warranted that values publicly available information as much as, if not more so than restricted data. For the military, change will begin at entry-level education and training venues. "Digital natives," the next generation of intelligence professionals that has grown up with ubiquitous technology and social media outlets, will likely find it easier to break from legacy mindsets. However, the lure of the classified source will still be seductive. Intelligence training must support the next generation's inclination to reach for the open source.

Additionally, future Airmen will require training in the tools available at that time and encouragement to pursue their own innovative ideas to best collect and analyze open source material. Specific analytic training should include problem restatement, causal flow diagramming, weighted rankings, devil's advocacy, and many other techniques as described by Morgan Jones in *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving.*

The importance of teaching analytical techniques to Airmen for use with the avalanche of data cannot be overemphasized. First, these techniques allow analysts to "show their work," making their analyses transparent to others. Second, they teach language precision, forcing analysts to frame the problem correctly to ensure it is answerable and not open to interpretation. Last, they can prevent military analysts from falling into the System 1 trap that Kahneman describes. The natural human inclination to grab onto the first plausible explanation is a key challenge for anyone, but especially for intelligence professionals confronted with the time constraints of military operations.

Those in leadership positions will often seek data compatible with the beliefs they already hold. Normally, in military operations, this means a desire for classified information over less glamorous open sources.[46] One way to break free from this confirmation bias is to use skills inherent in applying appropriate analytical techniques. With these skills and knowledge, the IC will be able to better respond to decisionmakers, rather than wasting time and effort on mundane production quotas endlessly seeking puzzle pieces.

If the IC is serious about developing critical thinking skills, the right answer is not to dismiss these analytical techniques out of hand but to experiment in accordance with proven scientific methods. Tetlock notes, "The intelligence community's forecasters have never been systematically assessed" to determine the accuracy of their analytic predictions.[47] Were the IC to do so, the entire test would be relatively inexpensive compared to the cost of flying and maintaining ISR platforms. Looking at the results of an open source–based experiment could provide valuable, low-cost information that might better enable future planning and budgetary decisions.

But what to do with "legacy" intelligence analysts? Individuals born prior to the Information Age may be less welcoming of open source material and more disposed to favor traditional sources of collection. But rather than endure the slow movement of time while the next generation ascends to leadership positions, forward-thinking military analysts must break from the classification fixation now. They must realize the relevance of open sources to guide collection, not the other way around. Additionally, individual analysts must *want* to contribute. But how?

The Intelligence Advanced Research Projects Activity (IARPA) is an Office of the Director of National Intelligence–sponsored program that challenges participants across the IC to engage in forecasting competitions. A spinoff program called the Good Judgment Project involves any willing participant both inside and out of DOD. The first IARPA tournament began in 2011 and explored the potential of crowd-sourced intelligence. Participants made predictions about real-world events, which were then judged by the precision of their forecast. Perhaps the most interesting outcome of the Good Judgment Project was that individuals with access to restricted information had no advantage over those without. In fact, the opposite was true, possibly due to the cultural bias toward classified information that may have prevented those individuals from forming more holistic predictions. In a *Washington Post* opinion piece detailing the competition's results, David Ignatius specified that individuals *without* access to classified information "performed 30% better than the average for the intelligence community analysts who could read intercepts and other secret data."[48] He continues, "The NSA [National Security Agency] obviously operates on the theory that more data are better . . . but this mad dash for signals lacks the essential quality of sound judgment."[49]

Just as the military stresses physical training (PT) culminating in regular tests, so should DOD champion regular "cognitive PT" tournaments. Results from multiple Good Judgment Project competitions revealed, "Prediction accuracy is possible when people participate in a setup that rewards only accuracy—and not the novelty of the explanation, or loyalty to the party line."[50] In other words, competitions like these foster both creative and critical thinking while honing skills on an individual level. Furthermore, competitions may lend themselves to developing and asking questions that can be answered, measured, and scored. Competitive events are not new for the military. For decades fighter pilots have trained against rival squadrons during "turkey shoot" events. Winners receive accolades and the recognition of their peers. DOD needs an open source–focused ISR turkey shoot, challenging participants to form their own conclusions based on publicly available information, thereby granting agency to the individual and allowing motivated professionals to best demonstrate their analytic prowess.

Competition between individuals and units could spur motivation and breed further intelligence excellence. And based on the results of the Good Judgment Project, one might expect open source disbelievers to become converts. At a minimum, participants will learn that classified sources matter less than the rigor one applies to analysis.

Final Points—An Opportunity for Success

Future success in detecting ambiguous clues that may lead to conflict will come through the patient process of creatively analyzing problems and articulating viable solutions. The data feeding those solutions will increasingly be found in readily accessible, yet traditionally stigmatized, open sources. But as a former Operation *Enduring Freedom* senior intelligence officer wrote, "The intelligence community's standard mode of operation is emphatic about secrecy but regrettably less concerned about mission effectiveness."[51] Individuals must overcome the classification fixation and focus on the information that best leads to mission success.

Machines can assist the analytical process but they are not a substitute for it. "Machines may get better at 'mimicking human meaning' and thereby better at predicting human behavior,"[52] but Tetlock argued there is a significant difference between mimicking meaning and deciphering the meaning's original intent. He concludes, "That's a space human judgment will always occupy."[53] To that end we must invest in the human mind in the form of analytic training combined with predictive forecasting based on publicly available information. Targeted investments directed toward improving creative thinking and smartly leveraging open sources will ultimately assist leadership decisionmaking and give the IC a strong comparative advantage in the future. **JFQ**

Notes

[1] I wish to thank Colonel Jeffrey Donnithorne, Dr. Jon Kimminau, Dr. Lisa Costa, Dr. Robert Norton, Mr. Josh Kerbel, Lieutenant Colonel Robert Folker, and Majors Kyle Bressette and Seth Gilpin for their thoughtful comments and suggestions. All errors found herein are my own. See also Adam Lowther and John Farrell, "From the Air," *Air & Space Power Journal* 26, no. 4 (2012), 61–102.

[2] Marcus Weisgerber, "Dempsey's Final Instruction to the Pentagon: Prepare for a Long War," *Defense One*, July 1, 2015, available at <www.defenseone.com/management/2015/07/dempseys-final-instruction-pentagon-prepare-long-war/116761/>.

[3] Gregory F. Treverton, *Reshaping National Intelligence for an Age of Information*, RAND Studies in Policy Analysis (New York: Cambridge University Press, 2003).

[4] Josh Kerbel, "The U.S. Intelligence Community's Creativity Challenge," *National Interest*, October 13, 2014, available at <http://nationalinterest.org/feature/the-us-intelligence-communitys-creativity-challenge-11451>.

[5] Robert Baer, *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism* (New York: Crown, 2002); see also Bruno Tertrais, review of *The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy*, by David E. Hoffman, *Survival* 52, no. 1 (2010), 220.

[6] Treverton.

[7] Anthony Olcott, *Open Source Intelligence in a Networked World* (New York: Bloomsbury Intelligence Studies, 2012), chap. 6.

[8] Ibid., chap. 4.

[9] One problem with this process is that it results in poor metrics for determining intelligence, surveillance, and reconnaissance effectiveness. Civilian and military collection managers prioritize their collection requirements, derived from the National Intelligence Priorities Framework at the national level and command-driven intelligence requirements below that, based on the priority of the intelligence needed to support a given mission. Quantitative measures such as the number of missions tasked or the number of images collected and processed are often used as proxy measurements to evaluate the effectiveness of meeting prioritized collection requirements. These data are easy to numerically collect and aggregate, but they distract from investigating qualitative indicators that might determine whether the intelligence process is contributing meaningfully to solving the underlying intelligence problem. It also speaks to a failure both to critically analyze problems and to devise creative solutions. Lieutenant Colonel David Vernal, Air War College student, interview by the author, November 15, 2015.

[10] Graham T. Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis* (New York: Longman, 1999).

[11] Ronald D. Garst, "Fundamentals of Intelligence Analysis," in *Intelligence Analysis: ANA630*, vol. 1 (Washington, DC: Joint Military Intelligence College, 2000), 18–28.

[12] The difference between *descriptive analysis* describing who, what, and where questions and *predictive analysis* is that the latter does not easily lend itself to statements of fact, thereby inducing greater cognitive stress. Addressing predictive "what will happen" questions forces the analyst to assume more risk by making subjective judgments amid uncertainty. Moreover, these open-ended questions must be answered with a range of possibilities, often tied to equally subjective probabilities.

[13] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2013).

[14] Vernal, interview, November 15, 2015.

[15] Kerbel.

[16] Remarks by Central Intelligence Agency Director Michael Hayden, Council on Foreign Relations, Washington, DC, September 7, 2007, available at <www.cia.gov/news-information/speeches-testimony/2007/general-haydens-remarks-at-the-council-on-foreign-relations.html>.

[17] As Lieutenant Colonel Adam Stone identified in a 2016 Air War College study, the Air Force does not have the luxury of tapping into a wealth of critical thinking (CT) capability. Pointing to the Air Force Future Operating Concept's desire for the identification of critical thinkers and metrics to track critical thinking skills, Stone executed a quantitative CT research project. He tested a sample of professional military education students in residence at the Air Command & Staff College (ACSC), School for Advanced Air and Space Studies, and Air War College (AWC). His (statistically significant) results indicated, "AF officers attending ACSC and AWC were below average in CT skills when compared with individuals at the same academic level." See Adam J. Stone, *Critical Thinking Skills of U.S. Air Force Senior and Intermediate Developmental Education Students* (Maxwell Air Force Base, AL: Air War College, 2016).

[18] Olcott, chap. 4.

[19] Philip E. Tetlock and Dan Gardner, *Superforecasting: The Art and Science of Prediction* (New York: Crown, 2015).

[20] Kahneman.

[21] Joseph Nye, noting the challenges facing foreign policy analysts after the Cold War, described a mystery as an abstraction that does not lend itself to quick answers or easy analysis. See Joseph S. Nye, "Peering into the Future," *Foreign Affairs* 73, no. 4 (1994), 82–93. Secrets, on the other hand, are more defined problems that can be answered via espionage or technical means. They lend themselves to satisfying seemingly factual answers and descriptive analysis. However, in the future, as more data become publicly available, proper employment of human-machine collaboration applied toward the open source information environment may yield insights formerly reserved to classified sensors alone.

[22] This point was further supported in an interview the author conducted with Robert Norton of Auburn University. Dr. Norton described the potential of monitoring foreign weapon manufacturing through an adversary country's research and development timeline. He noted that foreign universities emphasize the need to publish in technical journals as much as American higher education centers do. Information concerning technical developments can often be observed slowly building and then rapidly disappearing, perhaps marking that a country has reached the appropriate phase of research to begin transitioning a capability to the operational test and evaluation phases.

[23] Olcott, chap. 4.

[24] Kahneman.

[25] Ibid.

[26] Josh Kerbel, "The U.S. Intelligence Community Wants Disruptive Change as Long as It's Not Disruptive," *War on the Rocks*, January 20, 2016, available at <http://warontherocks.com/2016/01/the-u-s-intelligence-community-wants-disruptive-change-as-long-as-its-not-disruptive/>.

[27] Ibid.

[28] Treverton, 9.

[29] Ibid.

[30] Matthew Harris, "Marketing with Instagram, the Fastest Growing Social Platform!" *The Medium Well*, February 19, 2016, available at <http://mediumwell.com/marketing-instagram/>.

[31] Alec Ross, "Industries of the Future," Carnegie Council podcast, March 10, 2016.

[32] Treverton, 6.

[33] Ralph S. Clem, "MH17 Three Years Later: What Have We Learned," *War on the Rocks*, July 18, 2017, available at <https://warontherocks.com/2017/07/mh17-three-years-later-what-have-we-learned/>.

[34] "What We Know So Far About the Passenger Jet Shot Down in Ukraine," *Foreign Policy*, July 17, 2014, available at <http://foreignpolicy.com/2014/07/17/what-we-know-so-far-about-the-passenger-jet-shot-down-in-ukraine/>.

[35] Ibid.

[36] Ibid.

[37] Weisgerber.

[38] Ibid.

[39] Michael Kofman, "Russian Hybrid Warfare and Other Dark Arts," *War on the Rocks*, March 11, 2016, available at <http://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/>.

[40] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt, 2015).

[41] This is especially true regarding finding asymmetries against a conventionally stronger foe.

[42] Steven Pifer, "Russian Aggression Against Ukraine, and the West's Policy Response," testimony before the U.S. Senate Foreign Relations Committee, Washington, DC, March 4, 2015, available at <www.brookings.edu/testimonies/russian-aggression-against-ukraine-and-the-wests-policy-response-2/>.

[43] "NATO Flexes Its Muscle Memory," *The Economist*, August 30, 2014, available at <www.economist.com/news/international/21614166-russias-aggression-ukraine-has-made-natos-summit-wales-most-important>; Dan Gonzales and Sarah Harting, "Exposing Russia's Covert Actions," *U.S. News & World Report*, April 29, 2014.

[44] "Rise of the Machines," *The Economist*, May 9, 2015, 18–21.

[45] Maryam M. Najafabadi et al., "Deep Learning Applications and Challenges in Big Data Analytics," *Journal of Big Data* 2, no. 1 (2015), 1–21.

[46] Kahneman.

[47] Tetlock and Gardner.

[48] David Ignatius, "More Chatter Than Needed," *Washington Post*, November 1, 2013.

[49] Ibid.

[50] Angela Chen, "Seeing into the Future," *Chronicle of Higher Education*, October 5, 2015, available at <www.chronicle.com/article/Philip-Tetlock-s-Tomorrows/233507>.

[51] Michael Flynn, Matthew Pottinger, and Paul Batchelor, "Fixing Intel in Afghanistan," *Marine Corps Gazette* 94, no. 4 (2010), 62–67.

[52] Tetlock and Gardner.

[53] Ibid.