Semper Optiones: 21st Century Intelligence

COL David Pendall, USA

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

There is no American airpower, space power, land power, maritime power, or international political power without the knowledge provided by US intelligence professionals. Intelligence (INT) serves well today, but most importantly, needs to be better in the future. The thesis of this contrarian article is that technology has enabled, and always will enable, many different ways—options—to "do" intelligence. Consequently, we should continually seek better ways of "doing," organizing better structures for, and leveraging of new insights to plan, collect, analyze, synthesize, present, and use the data and information we call "Intelligence" today.[1] Intelligence now, in the United States, means the congressionally-endorsed organizational missions, authorities, and capabilities to collect data and information to produce insight and trusted judgment to government and military leaders and policy

makers in support of decisions and actions regarding national security and protection of US interests globally. The ideal is to understand everything, all the time.[2]

In plain language, this article argues that today's Intelligence technologies, processes, and structures are now, or may soon be, inadequate for the future. Plain language obviates the need to use many US Intelligence buzzwords and buzz phrases, the competing lexicons of "unified information theory," or picking sides in those bureaucratic or academic battles, though interesting and handy they may be. This argument begins with the obvious and ends with the contentious in the movement from upstream (where data is created and captured) to downstream (where it is converted, exploited, and enriched for decision and action). Most importantly, the article continues with the examination of significant implications for defense Intelligence processes, structures, security, and viability.

Upstream

Everything collected by any sensor upstream can be transformed directly or indirectly into zeros and ones downstream and then be progressively organized for processing, whether it is exquisite, phenomenologically-centered data, or data from multiple sources. Once processed, the collection can be analyzed and exploited for some purpose. The purpose may be as mundane as a business *predicting* what individual consumers have a high likelihood of purchasing or as elegant as *predicting* the location and behavior of "high-value targets:" individual terrorists, money launderers, or the wealthy "whales" upon whom the gaming industry depends. The business of Intelligence is the business of knowing. Premiums are placed on predicting behaviors and future operating conditions with high degrees of accuracy.

As for upstream collection, if it can be done by us, it is also being done by others (sometimes to us); with both good and bad intentions. Adversaries generally have the same ability to acquire and exploit the same commercially and publicly available data as the US. Here's a sample of what's available upstream:[3]

- full-motion video and electro-optic imaging from space, taskable with high periodicity (revisit), emplaced through multinational commercial investments
- environmental sensing and weather interactions affecting ground, sea, and air mobility and activities
- cyber transactions across the Open Web (internet), Deep Web (high-end commercial, industrial and academic exchanges), and the Dark Web (usually illicit and criminal transactions)
- online persona and behavioral graphing with resolution to the individual and internet protocol (IP) levels
- space-based collection and visualization of physical structures and city-scale assessments and characterizations for the insurance and risk assessment industries
- mobile smartphone transaction and location data supporting traffic pattern analysis, density graphs, behavior patterns, and current demographic flows

- social media sentiment and trending data based on issue, interest, and intensity, which can be further resolved to demographic segment and social status
- global interactions of distributed actors, devices, and affiliations based on IP connections and commercially-captured internet traffic, collected by manufacturers and sold to data brokers and marketing ventures, usually from application-based automated reporting (application programming interfaces). Internet of Things ([IoT] "smart" devices) reporting is also included.
- still image and video object extraction, recognition, and characterization, including facial recognition and database comparison matching, as related to internet-scale image and video posts—in near - real-time

YouTube, for example, ingests 400 hours of video every minute and distributes 5 billion hours of viewing content each month. YouTube does not just host the video, but scans it, characterizes it, stores it, and indexes it for many purposes.[4] Facebook and YouTube often contain exploitable data—evidence—of criminal, or other, activities we may need.[5]

The data exist. Exploiting it smartly is where the advantage lies in this decade and beyond. It is because of the beneficial or nefarious dual uses, reuse, and repurposing of the ever-expanding open-data universe that US Intelligence must learn to exploit it for predictive use—and at speed and scale. Operational success will depend on the creation of prescient intelligence at the velocity of data creation. The rules of the collection game are changing rapidly. To keep up with the changes requires a continuously adaptive Intelligence system to create knowledge out of data. This is the Intelligence-value proposition.

Useful information is becoming ubiquitous. The information collected and made available through direct sale, commercial data brokers, marketing venues, and social media is also held by the major data-capture corporations with analytical chops (Amazon, Google, Facebook, and Apple). These entities could train existing algorithms (artificial intelligence [AI] in its various manifestations) or craft new ones (deep learning) to answer almost every basic national security or defense question today. It has become an urgent matter of organizing this openly-available data for national security use. Exploiting and enriching it with the incomparable insights and knowledge that only US Intelligence and its partners possess, is part of the future value proposition.[6]

In today's world, the fact of the collection of these data, and as a result, exposing behaviors, relationships, and artifacts within these data, is inescapable. The concern of society, therefore, is more reasonably centered upon the **use** of the collected data—for good or evil—rather than the simple, inescapable fact of collection, and permanent archiving itself. Prevention or subsequent punishment of abuse and purposeful **misuse** of data, by governmental and nongovernmental entities, is where the societal concern should be. The sanctity of privacy and freedom in a world driven by the ubiquity of data and information on the individual is fundamental.

The logic of this model also holds that commercial and private entities may be much more adept, capable, incentivized, resourceful, and efficient in capturing and exposing data than any government entity. Therefore, the business of foreign intel-

ligence in the future will focus on the tailored assembly and synthesis of these globally-generated and available data (exploitation) for their intelligence consumers.

As we better understand, and begin to agree, that the information generated and commercially or publicly available today—a volume produced and stored digitally that is exponentially larger and richer than any in human history—the focus on information collection from solely government-developed, purpose-built, and "owned and operated" will diminish in overall merit and value.[7] We will move inevitably from an Intelligence culture dominated by vestigial beliefs and their associated behaviors reflecting information scarcity, excessive security, and a perceived disproportionate value placed on unique, singular contributions from large single-purpose workforces, INT bureaucracies and infrastructures, to one which embraces data abundance and a belief that "it's just data."

To exploit the upstream, the Intelligence culture will reflect a smaller, higher-end, integrated, and unified workforce, shared "back-office" services, and senior leaders who realize the profession ultimately exists to perform data synthesis and analysis, delivering meaning at the scale and speed relevant to decision makers and actors across all levels—tactical through strategic—simultaneously. The culture also must include public-private partnerships to further the development and exploitation of varied kinds of data; a pioneering pursuit presently being proposed by the National Geospatial-Intelligence Agency for geospatial information.[8]

In Transit

"In transit" has two aspects. The first aspect is the data moving downstream from sensor to a processor. The second, and profoundly affecting the first aspect, is the technological transit between now and the postquantum computing future. The logic of the model is that the three major entities pursuing quantum computing must be entities profiting from fast and increasingly accurate prediction: US Intelligence, on the one hand, but also the for-profit bodies like Amazon, Google, Facebook, and Apple on the other. (To murder a metaphor, the "third hand" is the academic and corporate communities that support the other two hands.) A major difference between the two hands is that Intelligence and their overseers are scrupulous and law-abiding: controlling the access and use of data in the best interests of national security. Commercial entities on the other hand—may not be as conscientious.[9]

Not all—read "only some of"—these forms of data and information require the same protection mechanisms that are currently afforded or were afforded in the last century to create competitive advantage. If the data in transit are encrypted, it may be an arduous and time-consuming process for a thief to render usable. If the data are unencrypted, theoretically any entity that can receive the data and immediately use the data. In the postquantum computing world, one may ask whether or not cryptography as we know it will survive. Our answer is "Yes, cryptography will

survive, but not as we know it." The issue raised here is a potential game-changer for all varieties of accessible data—at rest and in transit: US Intelligence may find it difficult to succeed in a world where the US is the fast second in quantum computing.[10] And that is second place in an unforgiving competition.

Downstream in Use

When the data arrive at the consumer and enter the consumer's associated processing workflows, the chore is to use it as rapidly as possible to discern changes and to make predictions. The further downstream use of the data is to comprehend the discerned relationships, and it is in understanding the patterns within the data that create competitive advantage. In business, uses include marketing-based information with the geospatial resolution of consumer patterns with retrievable buying and location histories, as one example. The data brokering of information on personal buying patterns and internet behaviors are bought, resold, and exploited in near- real-time for speculative action. Rarely do these business groups face mortal risks and consequences if their analysis is errant or their predictions are wrong. This is not so for intelligence professionals.

In intelligence, an army of people—subdivided into large and small groups, distributed globally (including aloft, afloat and submerged)—simultaneously need "just-right" information extracted from a mind-boggling mass of data every moment. The requirement to understand everything all the time begins with parsing the "everything" to focus on the sets of things—changes, movement, people, technologies, and so forth—that US forces and decision makers need to be knowledgeable of—right now.

Future Implications

In the future, the differences across Intelligence organizations should only be defined by the creativity and sustained pursuit of the advantage they can muster for their customer. The customer defines the end purpose or use (for good or evil) of information. The customer is agnostic to the original source and processing of single streams of unique data, much of which is losing its value as a distinct element. Simply stated, the source is irrelevant so long as the data is accurate. Single-source classified data, its legacy use, and its assessed value stemming from classified collection systems are rapidly being both rivaled and supplanted by an exploding universe of ubiquitous, commercially captured, common, and commoditized data.

For much of the emerging data, we do not yet fully understand its current value for defense intelligence or potential future uses. Before 9/11, we would not have associated anomalies of pilot training and one-way tickets. Similarly, we cannot fully develop smart insights among disparate data such as timber prices, cardboard boxes, and electronic product launches. There are insights to be educed. The value of collected and curated data, or its application, is difficult to predict. Some uses and analytic frameworks (tailored algorithms) have not yet been invented, and others already in use will evolve. As it evolves, the intense competition for data scientists and data curators will leave Intelligence and its supporting industry without

the full complement of the right human talent. How to hire, develop, compensate, and retain this type of talent must be addressed.[11] Perhaps outsourcing much of the workforce to a commercial firm with the ability to do this offers a solution. If so, Intelligence needs to rethink what its core functions and competencies really are in this century. We have moved from an industrial age to an information age, which requires new models for operating, teaming, and thinking that are dynamic to needs, time, and data creation. The industrial-age world was organized to perform linear processing and interrogation of hard-to-acquire, scarce data. In the twenty-first century's digitally integrated and dependent societies and nations—where quintillions of data bytes are generated daily—the processes must move from the linear to the nonlinear, commodity-based extractive model, and be as flexible and agile in this exploitation as is the dynamism of the emergent requirements and tempo of competition.[12] We often don't know what we need to know, until it is too late. We continuously incur global risks because of a lack of knowledge or understanding. In Intelligence, too many of our "analysts" are merely "processors" of data who are inadequately supported by insufficient automation. Worse, some parts of our Intelligence community seem satisfied with the status quo.

Technological Implications

The value created from data is centered on the conversion step that transforms it into an understood format. The transformation from a unique format to an enterprise-wide compatible and intelligible format is the point where a disproportionate value is created.[13] This point is where data can be of value to a wide range of applications. It is this step that commoditizes the data—placing it into the broader data universe, thereby allowing correlation, synthesis, pattern exploitation, and given the right algorithms, predictions.

Transforming signature data from discrete stovepipes and unique formats—understood by few—into commonly understood formats, across a data universe available to many, magnifies its value. Commercial data brokers and application makers know this and this is why data capture and marketing for future use and reuse are so lucrative. It is also one of the reasons that Amazon, Google, Facebook, and Apple trade at such high values: The *stored value* of that which they possess and the combinatorial potentials of what might be possible with such data. Technologies such as Blockchain and other distributed information and transaction security technologies, potentially contributing to creating this assured data universe for Intelligence, and further protected by quantum cryptography, may hold promise.

The material acquisition community (and defense contractors), military, and defense budget process managers, will need to adapt because this means an end to industrial-age procurement practices. This change disrupts current processes because it is not calling for large system procurements and programs to sustain "stuff"—sensors on platforms, multiple sea and air fleets, motor pools of ground platforms, maintenance shops, logistics, services, and so forth. This model is the opposite of that of the industrial era of mass and mechanical machines. Humans and machines communicating through algorithms is poorly understood and will initially be disruptive

to Intelligence. Nonetheless, recall the world leader who asserted that the control of AI would be crucial to global power?[14] AI control and quantum computing are our generation's race to the moon.

Organizational and Operational Implications

To the extent one believes Intelligence as a whole has made great strides under the leadership of James R. Clapper, had he continued to serve, he would have possibly continued to transform and integrate the Intelligence community.[15] To continue the transformation, as directed by its executive leaders, supported by its legislative overseers, and led by the US director of national intelligence, US Intelligence should be summoned to "start with the easy stuff:" organizing and centralizing the business processes of finance, acquisition, security, infrastructure, information technology architectures, and human talent management as the first steps toward dismantling "The Stovepipes" and recreating Intelligence. These modest business process reformations will be disruptive to some and gut-wrenching for many, but they are not only the barriers to exit from the present archaic and antiquated model (being kept alive by old laws and life support), but also barriers to entry into a revitalized model that puts analysis—and the human analyst—and human creativity at the forefront.

At the vanguard of the critical-for-differentiation-and-survival thrust in a new model, there needs to be an organizational blueprint that creates a data acquisition team, a data curation team, a data exploitation team, and a data visualization and distribution team apart from the existing phenomenologically-conditioned INT structure.

The data acquisition team is continuously scanning the information available and emerging from commercial and public sources and create the legal and practical mechanisms to bring these data or data accesses into the Intelligence architectures and workflows. The main consideration will be the data's use and relevance in supporting foreign Intelligence missions.

A data curation team is charged with reviewing and rating the internal qualities and veracity of the data itself, including its pedigree, source quality, and inherent flaws and use limitations under policy and legal statutes. Importantly, it is also the leader of the information assurance function.[16]

A data exploitation team should be empowered to design and create algorithms that deliver what lower- and higher-level analysts demand from their communications with the artificial intelligence in machines: knowledge of the present informed by the past and increasingly accurate predictions regarding the future. They should understand the flaws, implications, veracity, and composition of the data and data synthesis they create. A major component of the new organization's value will be its ability to create decision-quality information from smartly designed data models and algorithms (informed by domain team input) that work at enterprise/global scale and speed, producing competitively advantaged insight.

At the capstone, there needs to be a conscience: a data solution, process challenge, and innovation team. This team is the keeper of the current process/framework models and are also the "red teams," capable of and empowered to challenge

existing frameworks and the maturing data synthesis processes. While understanding and advocating for the organization's methodologies/tradecraft, they are simultaneously always looking for the outliers and "one-off" examples that current methodologies/tradecraft missed or insufficiently addressed. They thoughtfully challenge the existing views. They offer and build alternative models. Some models will be adopted and become the mainstay and some will be retained in hold status. The innovation component will be scanning the horizon for new data sources, emerging exploitation techniques, the creation of new best practices, and deeply evaluate the latest information science and technology trends.

All the teams—and their fixed and mobile elements, in the archaic terms of "forward and rear"—must be linked digitally and effortlessly into domain reference teams with depth and data on the history, economics, politics, demographics, ideology/culture, "military capabilities," and organizational behavior of other nations and rivals or potential rivals.[17] This group must be linked to the "conscience," engaged and contributing to the models helping humans discern and deeply understand "how things work" in the practical, physical, and human worlds.

There should be mutually supportive and explicit relationships among the domain reference teams and the data exploitation teams. Whenever the data exploitation team's views (or algorithms or results) diverge from the domain team's views (or algorithms or results), a deeper evaluation must be conducted to understand both "why" and also "how" to modify the algorithms that contributed. This evaluation is an especially important feedback mechanism to produce better insights and learning for the future performance of the organization and its ability to create meaningful and actionable knowledge—its central purpose. The logic of the model demands, multidata synthesis, and exploitation generate meaning and implications for decision and action. Single-data sources can complement or tip/cue data acquisition teams or data exploitation teams to adjust their acquisition or algorithms.

The workflows and familiarity of the production factory "task, collect, process, exploit, post" process must transform into an "access, synthesize, exploit" sequence. This sequence is tailored and decentralized, heavily dependent on domain awareness and team-based collaboration. It is not an industrial-age, assembly-line process or a linear assembly of resultant facts for a fixed report or product, but a synthesis of multivariate data and the tailored exploitation of meaning for a desired outcome and consequence that lives inside decision tools and the visualizations of future conditions. The interconnected world and the speed of interaction make it necessarily so.

Due to the complexity and the interdependence of people and things in the twenty-first century, there will be no single-source monopolies. All behavior creates a multitude of unique data (signatures) in the data universe. This data will either be directly sensed or enabled/made observable through correlated proxy data, providing the context, meaning, and implications. Finding the right signals in the noise of this man-made universe is dependent on the consumer's stated or discerned use of the data. It will vary as the needs of the consumer change, and the problem to solve is identified and clarified. Asking the right questions matters, correspondingly, to the qualities of the answers.

As far as the protection of the data itself—or the "fact" of collection—it exists and will in greater amounts and varieties whether we like it or not. It is, and will always

be, accessible to a wide variety of consumers, exploiters, brokers, or other entities (seeking to both good and evil). The very idea of "protection of sources and the collection capability" may not hold in the twenty-first century.[18] No longer will the protection requirements be in the form of protecting the fact of original collection, but must be applied to the intended and actual use of the data.[19]

Twenty-first Century Competitive Advantage

In this century, we have rediscovered, through aggregated data and the ability to find once hidden patterns and relationships in the data, that there are many interdependencies and signatures created simply from positive (or even passive) existence. We have also found that any single-sourced view into a phenomenon or activity is likely to miss more than it discovers or illuminates. That is why the twenty-first-century model must synthesize and exploit multivariate data from the points of collection earlier and faster in the workflows, assessed and expressed coherently, to orient the decision frameworks. Without this, decisions are likely susceptible to bias, deception, cumulative risk, and an artificial sense of certainty.[20] There is no 100 percent certainty in any man-made framework, but the old model is less capable of producing higher fidelity and veracity than the model for the near-future proposed here.

The goal is to develop a data acquisition and exploitation framework supporting a sense of reality that allows the organization to maintain a level of unrivaled competitiveness. This means a posture that surpasses the other competitors by supporting better decisions and actions at the tactical through strategic levels in a given field of competition. In a way, this is the twenty-first century OODA (John Boyd's "observe, orient, decide, and act") loop, enabled by the digitization of data (all zeros and ones). It is the observe phase that results from the collection of relevant digitized data, fed into organizationally tailored algorithms, processed into meaning (creating organizational orientation), and then fed into the decide and act frameworks. This phase is done at all scales and speeds, aggregated and disaggregated, continuously. This is less a schema to *predict* the future, although it will contribute, but rather one to help *create* the future. The future is created by providing the capabilities to navigate unfolding circumstances, wherein the winner maximizes competitiveness, the value of decisions, and the consequence of actions, while reducing risk and the chances of catastrophic failure or inexcusable setbacks (for a business and organization of the nation).

In our future, identifying the emergent need is essential for understanding at the speed of competition. To achieve this, the universe of data must be mined, exploited, synthesized, and presented at a speed and scale offering an advantage in decision and action, relative to actors who compete against us or are preparing to harm us. This—no harm—is the inescapable imperative. The need for an understanding of specific conditions, relationships, actor intent, and emergent potentials is what drives the clever data collection, extraction, and tailored assembly into useful insights that maintain our competitiveness. Clever means the ability to disproportionately or efficiently monetize, act, retain options, or otherwise smartly maintain an

advantage, whether these competitive behaviors occur in the market or for the national interest. That specific need for relevant data may be identified by a human—or more likely—an algorithm (human-built or, increasingly, machine-built) and will be occurring continuously and globally, at the speed of light (input-process-output-repeat). It may well be that Intelligence will get more value from commercially available information in the future than what it collects on its own today. The use of the commercially available data it accesses may create faster, more usable, and more important insights than Intelligence produces today.

The very idea of single INT supremacy or a single INT having a disproportionate influence or value in contributing to understanding is based on an industrial model and linear processing frameworks.[21] As with discoveries in investing, there are no single trend performance data across investment classes and assets that carry the day in making decisions. Collectible multivariate data generated from sensors capturing meaningful behaviors or "facts" of physical existence or "being" (location, material composition, dimensional properties, and so forth) will have strong correlations and tendencies to move together in ways that provide insight to those who are aware (and have the frameworks to create awareness). At the same time, there needs to be a set of data monitored in the same domain that is uncorrelated or has not followed the trends as another veracity metric, to balance the risk of taking too strong of a position (analytic judgment) on an unfolding set of circumstances or to reinforce the position (analytic judgment).[22] The most informative data sets balance correlations and trending across interdependent data streams to inform the decisions about what to do or how to act for advantage.

Since much of the data is generated by "social" interactions—whether it is the interaction of devices, machines, humans, or organizations—the creation of one's reality and the future is largely through the ability to integrate and interpret the data. One's view of the world becomes dependent on what information portals and personal interactions to which one has access. Whether one's world view is really an "echo chamber" or shaped by a refined and broadened set of inputs, it will still be subjective and limited. Objective truth for a human or an organization is a myth, which is not to trivialize the power of either faith or hope, while simultaneously rejecting the inappropriateness of myth, faith, or hope as lifelines for national security. Hence, the conclusion is that re-thinking our options for recreating, and then recreating Intelligence, would be a singularly valuable contribution to our national security. Even if we reject challenging today's structures and models, there are few forces beyond bureaucratic inertia that make it likely that the single INT, separate INT, structure will exist two decades hence.

Conclusion

Let's close with a thought from Edward Teller and a question for honest reflection. Teller observed that "The past is done. Finished. The future does not exist. It must be created microsecond by microsecond by every living being and thing in the universe."[23] We are cocreating the future of Intelligence, and hence US military and US global power, even as you read this.

The AI and quantum revolutions create the twenty-first-century arms race that is being pursued by our most capable adversaries. They will have no mercy in exploiting these arms and weaponized data, creating a future whereby our national security and elements of national power are undermined. Absent our recognition of this and a political will to make significant change ahead of this already unfolding curve, we will see our future disadvantaged. It is the fast-moving train we need to step onto, even if that means leaving some of our baggage behind. We know our adversaries are already ticketed and preparing to jump on (or are already traveling on) this train.

The reality of continuous co-creation begs a question to my sisters and brothers in the Intelligence profession—and to you, the ones whom we proudly serve. That is, "To what degree has Intelligence embraced the October 2004 summons to find ways of bringing *creativity and imagination* back into the Intelligence business and, more importantly, what more should we be doing?"[24]

Rest well, teammates. We never sleep.[25] ✪

Notes

1. The capitalized "Intelligence" refers to the apparatus and the product of present and future entities providing the information and insights essential for the preservation of our nation's security. The lower-case "intelligence" describes the activity of exploiting information for less lofty motives.

2. Our nation should choose better ways to understand everything all the time, not just because we can, but because we must. Some of these methods require learning from "intelligence" in business. Business intelligence is analogous although collection may be narrower, and the objective is to monetize insight.

3. A collection of capabilities regularly covered in industry and Intelligence open-source forums and public literature.

4. Armed Forces Communications and Electronics Association Europe Stockholm Chapter, "Google Federal Cloud presentation" (presented at the Technet Europe 2017 conference and expo, Stockholm, Sweden), 9 October 2017.

5. "According to a recent survey by LexisNexis Risk Solutions of more than 1,200 law enforcement professionals with federal, state, and local agencies. 83% of the respondents are using social media, particularly Facebook and YouTube, to further their investigations. More than two-thirds (67%) of respondents believe that social media helps solve crimes more quickly." John Patzakis, "Five Case Studies of Social Media Evidence in Criminal Investigations," *Next Generation eDiscovery Law and Technology Blog*, 16 November 2012, https://blog.x1discovery.com/2012/11/16/5-case-studies-of-social-media-evidence-in-criminal-investigations/.

6. Tailored insight, decision support, and enablement for consequential actions are the keys to providing intelligence value. Because of the artificial intelligence (AI) component of our future, China, Russia, and even well-financed transnational criminal organizations may possess nearly the same abilities.

7. Commercial entities currently seem better poised than the US government to collect and assemble big data. Consider: (1) how to protect/defend against the illicit use or adversary access/use, (2) how to prevent commercial entities from nefarious use or abuse, and (3) how does the intelligence community (IC) access this commercially created/collected data for national security? (Consider Apple: they are building their entire business on the sanctity of the personal data of their users. This is why they would not cooperate with the IC in accessing the San Bernardino, California shooter/terrorist's iPhone.) The author thanks COL Ron Corsetti, USA, for several key observations and suggestions throughout this article.

8. National Geospatial-Intelligence Agency (NGIA) Director Robert Cardillo made these remarks at the 2017 GEOINT Symposium, 5 June 2017, https://www.nga.mil/MediaRoom/SpeechesRemarks/Pages/GEOINT-2017-Symposium.aspx.

9. This was as demonstrated, for example, by the sale of advertising to US adversaries in the 2016 election and supporting the simultaneous concoction and dissemination of multiple fictions helpful to adversary interests, both of which must be judged as being less than conscientious. The judgment on entities like the Office of Personnel Management and Equifax is that they lacked the diligence to operate in a connected world of rivals.

10. Consider the protection of data at rest and the fragility of AI algorithms. An AI algorithm will only work well if the quality of the data can be assured. Otherwise, the algorithm will break. If the data is good in the first place, how can it be protected from accidental or purposeful corruption?

11. This would—because it must—include more clever and appropriate policies for duty location and flextime, geographic assignment, professional development, student loan payback, family leave, acceptance of diversity, and other human needs presently un- or under acknowledged. Worse, the multistovepiped Intelligence members may begin to "fight" with one another to acquire the same human talent.

12. More than 3.8 billion people interact on the internet daily and millions of self-synchronizing smart devices are added daily. These numbers are growing and in 2017 the data generated daily is measured in hundreds of "quintillions." The US alone generates more than 2.5 billion gigabytes per day. We will need to make up new measurements for the data by 2020. Tom Hale, "How Much Data Does The World Generate Every Minute?," *IFuc***gLoveScience*, 26 July 2017, http://www.iflscience.com/technology/how-much-data-does-the-world-generate-every-minute/.

13. Once a bit or byte moves from a form that can only be understood by a unique processor and is transformed into a format understood by a broader community of applications, machines, or humans, it has exponential value and use.

14. David Meyer, "Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World," *Fortune*, 4 September 2017, http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/.

15. Robert Cardillo, who for the past three years has led the NGIA, probably has a better sense than most as to the "what comes next" for intelligence, having worked very closely with former Director James R. Clapper. Consequently, it would be prudent to developments in NGIA to anticipate what comes next. Among what is observable so far are: importing talent from other intelligence agencies and—more importantly—the world of commercial technology to fill high level NGIA positions; building and strengthening global military partnerships; creating formal and informal networks of commercial affiliates; rationalizing personnel policies and practices; creating an empowered organizational structures; prototyping products created only from open sources; expanding the intern program; creating a "Ventures" office to accelerate innovation; and, jump-starting computational thinking, coding, machine augmentation for analysts, and beginning to sortie into the world of AI.

16. If the data cannot be assured and protected from corruption, manipulation, and so forth, the artificial community will break or become unreliable.

17. Little today is effortless for the human analyst, and too much is brute force or manual workarounds to access and share enterprise data.

18. The counterintelligence functions include understanding how the data may be exploited, who is acquiring the data, and understanding adversarial data transactions. Both nation-states and nonstate actors (transnational and domestic) have the means to leverage much of the same data for their own uses and advantage.

19. The protection of data in the past was also related to the loss of value if it is compromised (we spent X during Y years to acquire it and its resultant data stream in world of information scarcity), and now that the unique source is compromised, we lose the source and any future value it could produce. Loss regret is also related to the "shame" factor—whereas, individuals or organizations would be shamed or embarrassed if the artifacts or knowledge of their behavior were made public, accepting that what does, or should, shame varies by culture and by generation within a culture or peer/reference group. Privacy was valued, transparency was a risk. The loss of individual or organizational privacy could mean lawsuits, prosecution, loss of status, liability for harm, or other penalties, not to mention the loss of trust. Also, these perceived negative consequences imply socially or could legally determine the behavior was not something acceptable in the social or legal frameworks within which the individual or organization operates. As far as the "cost" of compromise of a unique source when a target becomes aware of the collection capability or method and changes its behavior or institutes countermeasures—

that may still happen, however the multitude of commercial and other data collection existing reduces the overall value of unique sources and provides a wide variety of both direct and proxy data that illuminates the targeted entities activities, relationships, intent signals, and other strategically, though tactically relevant, data for decision and action. Even crowd-sourced, socially exchanged data will contribute to an understanding of threats or adversarial intent.

20. "Machine bias is human bias," according to Daniel Newman. *See* Newman, "Your Artificial Intelligence Is Not Bias-Free," *Forbes*, 12 September 2017, https://www.forbes.com/sites/danielnewman/2017/09/12/your-artificial-intelligence-is-not-bias-free/#5d879ef8c783.

21. As realists, we accept that some aspects of single intelligence capability will persist, much like the Panda's Thumb or the QWERTY keyboard. The National Reconnaissance Office (NRO)—a very large "office" indeed, self-described as a "hybrid organization consisting of some 3000 personnel"—for example, cannot conceive of a world without an NRO. Others can easily envision such a world. See http://www.nro.gov/about/nro/who.html.

22. The late Alvin Toffler cautioned that watching trends for their predictive power was inadequate since it may very well be that the countertrends are the ones that create history.

23. Air University, *SPACECAST 2020 Final Report* (Maxwell AFB, AL: Air University, 22 June 1994), http://www.au.af.mil/au/awc/csat/2020/monographs/process.pdf.

24. "National Commission on Terrorist Attacks upon the United States, *Report of the 9/11 WMD Commission* (Washington, DC: 9/11 Commission, 1 October 2004), 20,410.

25. As Tom Greco, G2 for US Army Training and Doctrine Command, remarked, "Actually we do, but AI doesn't have to!"

COL David Pendall, USA

Colonel Pendall (MS, Army Command and General Staff College; MA, Central Michigan University; BA, Ohio University) is the deputy chief of staff for Intelligence (G2), the senior intelligence officer for the US Army–Europe (USAREUR). He was commissioned in 1990 through the Ohio University Army ROTC Program. Colonel Pendall was also an Army War College Fellow at the Massachusetts Institute of Technology's (MIT) Security Studies Program in 2012–2013. Previous assignments include service with the 11th Armored Cavalry Regiment in Fulda, Germany; battalion and brigade combat team intelligence and security positions within the 1st Cavalry Division (CD); commander, Company A, 312th Military Intelligence Battalion (MIB) (Operation Joint Forge), Multi-National Division-North, 1st CD; officer-in-charge of operations and training, 741st MIB; strategic planner, National Security Agency, Signals Intelligence Directorate; Joint Staff strategic plans and policy planner, US Central Command Forward; intelligence planner and analysis and control element chief (ACE), Multi-National Corps-Iraq; USAREUR ACE chief, 24th MI Battalion/66th MI Brigade; USAREUR intelligence, surveillance, and reconnaissance plans chief, intelligence plans officer; North Atlantic Treaty Organization/International Security Assistance Force Joint Command Headquarters; senior intelligence officer, Combined Joint Staff Branch for Intelligence, Regional Command–East, concurrently serving as the 1st CD G2; and the Department of the Army G2 liaison officer with MIT Lincoln Laboratory. His deployments include Bosnia–Herzegovina, Qatar, Iraq, Turkey, and Afghanistan. The colonel's preceding assignment was commander, 66th Military Intelligence Brigade.

Distribution A: Approved for public release; distribution unlimited.

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