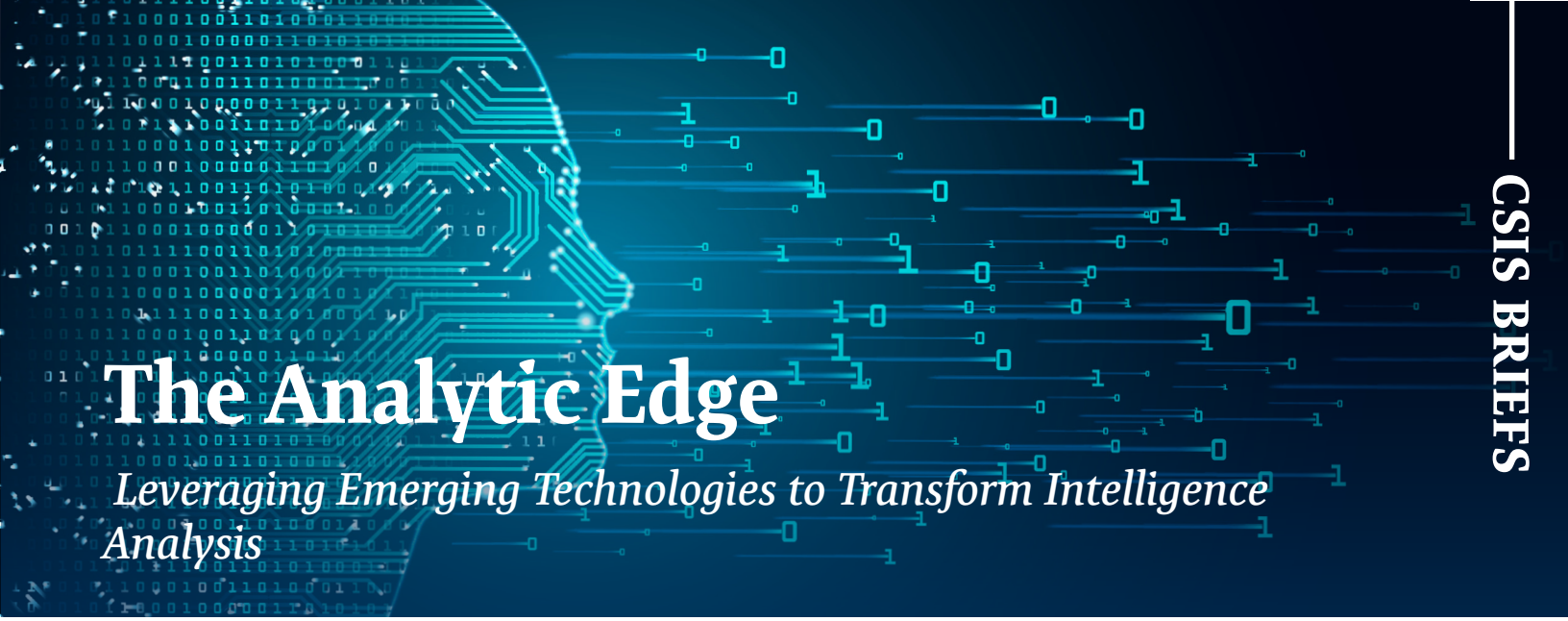

CSIS BRIEFS

The Analytic Edge

Leveraging Emerging Technologies to Transform Intelligence Analysis

By Brian Katz

OCTOBER 2020

THE ISSUE

- **How well and how rapidly the intelligence community (IC) integrates emerging technologies into all-source analysis will be vital** to its ability to generate timely, relevant, and accurate strategic insights and to sustain policymakers' decisionmaking advantage over capable rivals.
- **Artificial intelligence (AI) and associated technologies cannot replicate all the complexities of crafting strategic analysis** but can automate, enhance, and enable key parts of the analytic process and be used to unlock new insights to inform analytic judgments.
- **AI can assist analysts in streamlining and sensemaking of exponentially growing intelligence data.** With fewer tasks, better data, and machine-derived insights, analysts will have more strategic bandwidth to apply their expertise and deliver high-level analysis to policymakers.
- **To harness advanced technologies, IC analysts must overcome a host of challenges, barriers, and limitations**—in the underlying data, algorithms, and ultimately the analysts themselves.
- **IC leaders and stakeholders—policymakers, Congress, the technology, and research sectors—must provide the analytic workforce the technology and training to thrive today** while laying the digital groundwork, institutional priorities, and cultural norms for future success.

INTRODUCTION

If the United States invests now in technology transformation, the intelligence analyst of 2030 will be able to look back at the analyst of 2020 with incredulity and even pity. Armed with world-leading AI, cutting-edge data analytics, and unlimited cloud computing power, the analyst will maintain almost continual awareness of their target operational environment. They will rapidly surface, fuse, visualize, and action high-quality data across the information spectrum, from open-source to highly classified. They will deliver high-level, data-rich, quick-turn insights to their policy customers. The analyst will shrug at their predecessors' ad hoc adoption of technology and antiquated "read, write, think" analytic process as relics of a bygone era that is incompatible with the speed and scale of big data.

The analyst of 2020 has neither the time nor inclination to ponder this seemingly fantastical future. As data grows exponentially, their capacity to process it grows marginally. Their monitors are filled with multiple intelligence queues, siloed share drives, manually curated spreadsheets and databases, and error-riddled .kmz files, with no interface to synthesize the data. They are overwhelmed by myriad new tools and "AI solutions" now offered to them and

underwhelmed with their utility and suitability for strategic analysis. With unrelenting customer demands and timelines, the analyst defaults to their small set of trusted compartmented sources and time-tested tradecraft to assemble their evidence and deliver a "good enough" intelligence product that is more or less on time.

While the current picture is not as bleak and the future likely not as optimized as above, IC analysts in 2020 are flatly behind the technology curve. The explosion of data and disruptive technologies, rapid evolution and emergence of new global threats, and accelerating policymaker decision cycles will likely upend the intelligence analysis process. How well and how rapidly the IC integrates advanced technologies into all-source analysis will be vital to its ability to compete in future intelligence environments and deliver timely, accurate, and relevant analytic products.

While envisioning and building towards the analyst of the future, the IC can and must harness emerging technologies to empower analysts today. In part two of its three-phase study, the CSIS Technology and Intelligence Task Force explored how technologies such as AI[1] and its subset machine learning (ML),[2] cloud computing,[3] and data analytics can empower intelligence analysis. Building off phase one of the study, which focused on intelligence collection, the core research question guiding phase two was *what are the opportunities and limitations of emerging technologies for strategic intelligence analysis*? To answer it, the Task Force convened stakeholders and experts from across the IC, technology, policy, and research communities for a series of discussions.

This CSIS research brief summarizes the main findings from the second phase of the Task Force. The brief begins by studying the near-term ways technologies can be integrated into the analytic process. It then assesses the key barriers and limitations to integrating AI and other technologies into strategic analysis. The brief concludes by exploring where technology and analysts will provide the most value to policymakers and the implications for building the IC of the future.

OPPORTUNITIES: CREATING STRATEGIC BANDWIDTH

"The IC's job," as the ODNI AIM Initiative describes it, is to "analyze data, connect disparate data sets, apply context to data, infer meaning from data, and ultimately make analytic judgments based on all available data."[4] The problem, however, for analysts today is that "the pace at which data is generated, whether by collection or publicly available information, is increasing exponentially and long ago exceeded our collective ability to understand it or to find the most relevant data with which to make analytic judgments." If analysts cannot process, absorb, and integrate the right data, they cannot turn it into coherent, insightful, and compelling analysis for their customers.

AI and associated technologies cannot replicate all the complexities of crafting strategic analysis but can automate, enhance, and enable key parts of the process and be used to unlock new insights to inform analytic judgments. These technologies can help *optimize* intelligence flows, *automate* mundane but vital processing tasks, *augment* analysts' sensemaking and critical thinking skills, and even *perform* certain types of analysis. Emerging technologies can, in short, create more *strategic bandwidth* for analysts to think and write strategically. With more time, fewer tasks, better data, and new ways to generate insights, analysts will be more able to apply their unique expertise and deliver high-level, quick-turn, valued-added analysis to policymakers.

Optimizing Intelligence Traffic: The volume and variety of intelligence coming into analysts' "traffic" queues—from sensor data to signals intercepts to diplomatic cables to social media—has far surpassed what they can process. AI and analytics tools can help optimize information flows and augment and enrich them to gain more insight from less data in a fraction of the time.

- **Prioritized**: AI capabilities could be applied to triage and surface the most relevant and useful information prioritized by analysts, automating the time-intensive task of intelligence traffic curation.[5] AI tools could also be trained to scan, spot, and flag information analysts designated as critical or anomalous and prioritize it in their queues, providing early indicators and warning of new developments for analysts to alert policymakers.[6]
- **Personalized:** As AI-enabled traffic models learn analysts' preferences, AI prediction tools and recommendation algorithms could be used to find and flag reporting of interest based on the analyst's portfolio and search history (e.g., "If you liked that SIGINT intercept on Adversary Y, you might like this HUMINT report from Station X").[7] ML models could be honed for better customization over time, learning how analysts move through data and value certain report attributes which would lead to better recommendations.[8] Such reinforcement learning could extend across teams and agencies, leveraging cloud and collaborative filtering.[9]

AI and analytics tools can help optimize information flows and augment and enrich them to gain more insight from less data in a fraction of the time.

- **Summarized**: Advances in ML, particularly natural language processing (NLP),[10] could enable algorithms to comprehend and summarize large and growing bodies of unstructured text in intelligence traffic—HUMINT reports, processed SIGINT and imagery reports, diplomatic cables, and open-source—to trim and streamline traffic.[11] ML tools could help compress and even compose report summaries while identifying and clustering topics or entities of interest, enabling analysts to scan or dive deep into the reports as time allows.[12]
- **Enriched**: AI tools could be used to not only summarize intelligence but also to augment and enrich it, using automation to embed metadata such as time, location, actors, and events. Data enrichment could enable analysts to derive more information and context from each report and build connections across all reports.[13, 14]

AI and analytics tools can help optimize information flows and augment and enrich them to gain more insight from less data in a fraction of the time.

Smarter Search and Organization: After curating analysts' daily traffic, AI tools can assist analysts in how they search, organize, and begin making sense of relevant reporting. Technology can help analysts pose optimal questions, search the right datasets, and automate how data is collated and cataloged. By automating mundane but vital analytic tasks and better sifting "signal from noise," AI tools could enable analysts to move faster from structuring to sensemaking of data.

- **Intelligent Queries:** With AI, analysts could hone smarter questions and search algorithms for a given intelligence question, casting wider and more efficient nets across datasets to piece together critical but often nonexplicit information (e.g., what is adversary X's strategy for Y?). Analysts could team with data scientists to tailor how data is tagged (e.g., words associated with "strategy") and how queries are sequenced to enable algorithms to learn and launch more complex or indirect searches.[15] NLP applications could help summarize and structure the search findings based on specific analytic needs.[16]
- **Targeted Sifting and Surfacing:** With AI-tailored queries, analysts should be able to leverage ML tools to search and sift across vast and various datasets and reporting streams to surface intelligence of value. As results are filtered, NLP tools could help detect, extract, summarize, and gather prioritized information and topics—such as people, locations, organizations, and events.[17] Such sifting and surfacing capabilities could augment day-to-day traffic monitoring and searches but would be vital during times of crisis, helping analysts focus the intelligence flow, find the best data, and respond rapidly to policymakers' needs.[18]
- **Automated Curating and Cataloging:** Having gathered the right intelligence, analysts could exploit ML tools to automate the cataloging and organization of that intelligence. Instead of manually populating and integrating data spread across spreadsheets, databases, and .kmz files, analysts could harness NLP to generate "knowledge bases" that cluster, curate, and populate reporting into analysts' unique frameworks and ontologies.[19] Knowledge bases could be further automated to continuously analyze and self-update with new intelligence reports.[20]

Augmented Sensemaking and Detection: With intelligence sifted and streamlined, AI tools and advanced analytics could help analysts make sense of it, augmenting their ability to identify and visualize patterns, relationships, and change in their target environments in real time. Analysts could be able to leverage AI and cloud to maintain enhanced, persistent, and machine-updated situational awareness of their target.

- **Patterns and Networks:** With datasets pooled and integrated on cloud-based data lakes, deep learning algorithms[21] could be deployed to find patterns, trends, and relationships that would be impossible for analysts manually reviewing the data to identify.[22] Analysts and data scientists could team to develop and guide ML models harnessing neural networks to classify, cluster, and connect data into nodes and networks.[23] Applying ML to graph data—data that can be connected, like people, organizations, locations, and events, as nodes in a network—could enable analysts to not only identify relationships and networks but infer judgments on the key influencers and the nature of the connections, revealing new insights or validating initial assessments.[24]
- **Knowledge Visualization:** After identifying patterns and networks, analysts could leverage AI to visualize them for enhanced clarity, meaning, and integration into their

analysis. Synthesizing data from multiple data streams and analysts' internal knowledge base, AI tools could visually capture new intelligence and changes in their target environment.[25] With analyst-friendly interfaces, analysts could "see" their intelligence in compelling and manipulable formats and integrate it into creative products for their consumers.

- **Enhanced Situational Awareness:** AI and data visualization could enable analysts to eventually maintain a near real-time picture of adversary activity across multiple domains, providing a common operating picture (COP) that keeps pace with changes in the operating environment. Automating and orchestrating data display from various sensors, collection streams, and open-source intelligence (OSINT) in one interface could enable analysts to capture and monitor signals and data of new activity and establish patterns and baselines of what is routine and normal. An enhanced COP over time could provide a wholistic, dynamic accounting of U.S., friendly, neutral, and adversary activity and continual assessments of change for policymakers.
- **Detecting Anomalies and Incremental Change:** As analysts and machines team to establish baselines and expectations of adversary activity, AI tools could then surface anomalous behavior and detect weak but important signals and deviations to flag and direct analytic focus. By integrating analytic "tripwires" into monitoring frameworks, analysts could exploit AI for real-time monitoring of meaningful incremental changes otherwise missed in the daily intelligence churn and which can culminate later in strategic surprise and intelligence failures.

Offloading Analysis and Harnessing OSINT: AI tools could not only automate and enhance processing and sensemaking tasks for analysis but could also *perform* certain types of analysis. IC analysts can harness these tools and the growing availability, quality, and relevance of OSINT both to generate inputs and machine-derived insights for their analysis as well as to offload or outsource analytic work done as ably or better by machines.

- **Geopolitical and Battlefield Updates**: Analysts are called upon to craft daily "intelligence" products that update policymakers on political and military developments in conflict zones that are just summaries of media and other OSINT reports due to lags in classified collection. Analysts could leverage AI, particularly NLP, to cull the same data, summarize findings, and generate written summaries for analysts' updating, fine-tuning, and additional context.[26]
- **Stability and Crisis Monitoring**: Analysts could leverage AI-enabled data mining, sentiment analysis, and geolocation tools to help monitor and predict disruptive events—from mass protests to pandemic outbreaks—for early warning of potential crises and instability. When combined with data sifting, visualization, and NLP foreign translation tools, advanced OSINT capabilities could provide analysts a rapid and accurate initial assessment of global flashpoints and key indicators for where to steer classified collection.[27]
- **Political and Economic Forecasting**: Advanced OSINT could supplement or even substitute for all-source analysts in areas where the IC has a mixed tracked record of performance and unclear comparative advantage, such as predictive analytics and long-range geopolitical and economic forecasting.[28] Analysts could leverage their historic and classified knowledge of adversaries and machine modeling and compute power to generate sophisticated scenarios analysis, identifying high-impact but previously unforeseen scenarios and predictions.

Honing Analytic Lines: As analysts build their analytic lines, assembling key evidence and forming initial judgments, they could harness cloud, AI, and data analytics to refine and test their analysis against machine-derived and IC-wide insights. While unable to replicate an analyst's cognition, contextual knowledge, and critical thinking, AI can test and strengthen their analysis by surfacing contrary data, measuring historic accuracy, and positing alternative hypotheses.

- **Extended Intelligence Collaboration:** Cloud and AI tools can enable analysts to coordinate and collaborate more effectively from start to finish in the analytic process, from sharing and developing datasets and algorithms to jointly authoring products.[29] Analysts could reenvision coordination from simple product review to a collaborative process of *extended intelligence*, harnessing distributed human expertise with machine power to generate insights.[30] Collaboration could be extended not only across the U.S. IC but also with foreign liaison partners.
- **Testing Analytic Lines:** While building assessments, analysts can use AI and advanced analytics to test assumptions, hypotheses, and initial judgments against big data and algorithm-derived results. Corroboration

While unable to replicate an analyst's cognition, contextual knowledge, and critical thinking, AI can test and strengthen their analysis by surfacing contrary data, measuring historic accuracy, and positing alternative hypotheses.

could strengthen analytic lines while alternative findings push analysts to revisit their evidence, logic, and conclusions. As confidence in algorithms grows, analysts could use machine-derived findings to not only vet their analysis but inform it, leveraging new insights from data.

- **Overcoming Analyst Bias:** Machine knowledge and judgment of past analytic lines, source veracity, and competing hypotheses could add more rigor to analytic process while helping analysts confront bias and groupthink. AI could surface anomalous, undervalued, and countervailing reports that analysts trusting a small, compartmented source base may have missed or discounted.[31] Contrary analysis can help analysts overcome confirmation and anchoring bias on established analytic lines and instill more transparency in analysts' levels of confidence.[32]

Enabling Analytic Disciplines and Missions: AI and advanced analytics can be directly applied and integrated into core analytic disciplines and missions. These technologies can inform and enhance long-standing tradecraft in counterterrorism (CT), military, and political analysis and science, technology, and information warfare analysis rapidly rising in importance.

- **Targeting and Network Analysis**: AI, data analytics, and intelligence fusion tools could enable advanced network analysis for targeting operations and anomaly detection for "needle in the haystack" analysis vital to CT and other operational intelligence. ML and graph analytics could enhance any network-centric analytic mission, such as countering weapons procurement and proliferation, illicit trafficking, sanctions evasion, and transnational crime.
- **Military Analysis:** AI and multi-INT fusion and visualization tools could enable military analysts to build dynamic order-of-battle of foreign militaries and near real-time battle-tracking, bolstering insights on adversaries' strategic capabilities and current operations, including clandestine and irregular warfare activity.[33] AI and cloud could power advanced and more realistic war gaming and simulations. Deep learning and NLP could incorporate diverse datasets on adversary decision variables—from geospatial and logistics data to political intelligence and military doctrine—and integrate into decision models and courses of action.[34] Advanced simulations and modeling could augment war games of future scenarios but also day-to-day assessments of adversaries' near-term behavior and courses of action.
- **Political and Leadership Analysis:** ML, graph analytics, and data visualization tools could help political analysts structure and understand influence networks, "inner circles," and decisionmaking processes of foreign government leaders. Advances in sentiment analysis could allow analysts to better anticipate political trends and influencers shaping foreign decisions, while individual attribute modeling could help predict leaders' potential responses to various U.S. policies.[35]
- **Science and Technology (S&T) Analysis:** Much as analysts have long analyzed foreign weapons systems and defense industries, understanding foreign S&T innovation and integration into military and intelligence missions will be a top priority for IC analysis and policy customers for the foreseeable future. As IC analysts become more knowledgeable and adept at employing AI and other emerging technologies, their expertise could enable deeper insights and analysis of adversaries' S&T plans, intentions, capabilities, and threats. Tech literacy will be vital in assessing foreign cyber, disinformation, and influence campaigns and the implications of next-generation technologies, such as biotechnology and quantum computing.

LIMITS AND BARRIERS TO ADOPTION

While the benefits of AI and associated technologies could be immense for analysts, the IC faces several key obstacles and limitations in adopting and applying these tools to all-source analysis. The broad challenges of technology acquisition, digital infrastructure, and data architecture identified in phase one of the Task Force as hampering intelligence collection and processing missions will impact analytic missions as well. But structural barriers are neither the only nor often the primary obstacle. Prevailing against analytic adoption of emerging technologies is the technologies' own limitations in meeting analysts' standards of tradecraft and explainability, and the cultural

and institutional preferences of analysts and agencies for their traditional approach to intelligence and analysis.

Capturing and Integrating Data: Accurate and insightful application of AI requires capturing, cleaning, and curating the right data. The sheer volume of potentially relevant intelligence and data for analysis may surpass the capacity of even the most tech-enabled analysts to process, filter, and absorb. Further complicating the harnessing of data will be the challenges of standardizing and integrating the best datasets, both collected from classified means and surfaced from the open source.

- **Keeping Pace with Data:** The speed and scale of IC integration of intelligence and data processing tools must keep pace with accelerating volumes and diversity of intelligence and data. Even with AI-enabled optimization and streamlining, the proliferation of sensors, intelligence streams, and OSINT data—accelerated by 5G and IoT devices—could still overwhelm analysts' capacity to process. Inability to capture and analyze real-time data will leave IC analysts behind the curve in providing situational awareness to policymakers.
- **Integrating Data:** The best AI applications for analysts would harness both classified and OSINT data in training algorithms and deriving insights, but incompatible architecture and security barriers could hamper "low-side"/"high-side" data integration. Along with data, ML algorithms and models honed on open source could face similar obstacles being migrated onto classified systems and integrated into analytic workflows.
- **Tagging Data:** The best AI applications also require massive amounts of data, which in turn require extensive labeling and tagging—a tedious, time-consuming, and still primarily human task.[36] Unlike the private sector, which can crowdsource and employ "gig economy" taggers, the IC's classified datasets require labeling to be done internally and mostly manually by cleared analysts and contractors. While perhaps sufficient in the short term, manual labeling and tagging will be untenable as data continues to exponentially grow.[37]

Algorithmic Limits: Analysis depends on rigorous tradecraft and clear explanations and reasoning for the logic, evidence, assumptions, and inferences used to reach conclusions. The complexities of strategic analysis, standards and requirements for transparency and intelligence assurance, and the inherent challenges of modeling analytic processes and performance will create theoretical and practical limits to applying current AI capabilities to analytic workflows.

- **Modeling the Strategic:** The complex tradecraft and cognitive skills of strategic analysis is innately difficult to define, standardize, replicate, and thus model, creating practical limits for AI applications. Contextualizing and recognizing implications of new intelligence, weighing and connecting data to form an intelligence picture, organizing intelligence logically and persuasively into argumentation and assessments—the analytic process is a blend of art and science, standardized tradecraft and individual heuristics, and judgments derived from hard data and deductive reasoning and from cultural expertise and analytic intuition honed over time. If analytic tasks cannot be defined digitally, the ability to apply AI will be limited.[38]
- **Bias:** Generating insights from AI requires analysts to help shape, hone, and steer algorithms and models, but analysts introduce bias in how they conceptualize the intelligence problem, design the model, and select data for input, leading to biased and potentially inaccurate results. Transparency of biases inherent in the data, how models are used, and their impact on conclusion and confidence levels will be vital but may not easily be understood by customers.[39]
- **Explainability:** To use AI-derived findings, analysts will need to know the logic, bias, assumptions, and inferences of the algorithms and models used to generate them—which may or may not be knowable. Many of the most sophisticated AI applications and machine insights derive from "black box" algorithms in which machine logic and processes are hard if not impossible to define. A lack of transparency on evidence chains, where and how AI was used, and validity conditions means machine findings will be untrustworthy and unusable.[40]
- **Authenticity:** Analysts must continue to evaluate intelligence for its quality, accuracy, and relevance while learning how to measure a new factor once taken for granted: authenticity. Deception techniques to fool algorithms into misclassifying data and use of generative adversarial networks[41] to create deepfakes of classified and open-source data could sow confusion among analysts, leading to poor analysis and misinformed policy decisions.[42] Ensuring data and intelligence authenticity will only grow more difficult as adversaries become more adept at altering data and waging targeted disinformation campaigns at speed and scale.

- **Security:** Analysts will also face aggressive and targeted adversarial AI efforts from hostile foreign intelligence services aimed at penetrating and undermining AI systems—and with it, analysts' confidence in AI tools and results. The rush to adopt AI could come at the expense of rigorous AI security standards, protocols, and testing requirements, creating vulnerability to a range of "counter-AI" threats, from "poisoned" data injected into AI models to fully hacked and manipulated systems.[43] Even if adversaries cannot gain such a level of access, convincing analysts their AI is compromised and unusable could achieve the same effect.[44]

Analytic Aversion to Change: While the technical obstacles are significant and real, perhaps the greatest barrier to AI adoption could be analysts themselves. Deeply embedded in the analytic community are institutional, bureaucratic, and cultural preferences and bias toward the time-tested tradecraft and techniques they perceive to be the global gold standard. Underinvestment in digital acumen, uncertainty of AI and OSINT's mission value, and cultural aversion to risk and change could hinder even the most innovative analysts and units from integrating emerging technologies into their mission.

- **Digital Literacy:** Analysts will need baseline digital skills to effectively harness AI and analytics tools in their analysis and to explain AI-derived findings to even less digitally savvy policy customers. To develop those skills, analysts will need not only specialized training but supportive leaders and management that value and incentivize it. Agency leaders, however, will need to balance investment in digital proficiency with traditional tradecraft, language, and other regional-specific training that, too, will remain vital to the IC's analytic advantage.
- **Bureaucratic Disincentives:** AI investments require multiyear commitments to see through adoption and integration, managerial expenditure of social capital to gather institutional support, and leadership's acceptance of risk and occasional failure. Managers, however, are often only in their positions for 2-3 years and may be unwilling to spend their already strained time and resources on new technologies with uncertain mission payoff and a chance of failure, particularly if their IC leaders and oversight bodies do not incentivize such risk-taking.
- **Mission Value:** Training, incentives, and leader support may still not be enough to spark tech adoption if analysts and managers see no clear and substantial "mission gain" from the technology. Marginal gains in insights and productivity may not justify the time, expense, and opportunity cost required to gain AI and analytics proficiency. Analysts may also be offered too many technical tools to see the value of any, particularly those not specifically designed and tailored to their unique analytic needs. Analysts with trust and confidence in traditional tradecraft are more likely to discard ill-suited technologies than conform to them.
- **Trusting the Nontraditional:** Harnessing AI capabilities will require embracing OSINT as vital analytic input and learning to gain trust in machine-derived results. Blocking this embrace is an IC bias for classified reporting in forming judgments, skepticism of OSINT—only growing with deepfakes and disinformation—as diagnostic data, concern over AI security, and trust in time-tested tradecraft over black box processes. Preference for classified reporting may be appropriate, as a SIGINT intercept or HUMINT source may be the only way to discern plans and intentions. However, discounting timely, on-the-ground OSINT insight while waiting for clandestine ones to be collected and processed will leave analysts behind and outside policymakers' information and decision cycle.

OUTLOOK: TECHNOLOGY'S—AND THE IC'S—STRATEGIC ANALYTIC VALUE

In weighing its benefits and limitations, it is clear that emerging technologies such as AI, cloud, and advanced analytics can create more strategic bandwidth for analysts by automating and enabling key analytic tasks. But what is technology's value added to analysis itself? High-level analysis must answer the complex questions for policymakers (e.g., what are the prospects for conflict between an ally and rival power? Will mass protests in country X descend into civil war?). Answering them requires answering a series of interrelated sub-questions that must be connected into a coherent analytic story: *what* is happening and *why*, its *impact*, its *outlook*, and the *implications* for U.S. interests. Where can technology most assist in answering them?

Technology's immediate value is in answering *the what*—to capture, curate, connect, and make sense of vast streams of intelligence and data on what is happening with an analyst's country, issue, or target of interest. It can also help analysts assess *impact*—to detect and measure an issue or actor's impact on the operational environment. Where AI and associated technologies lag is in answering *the why*. Understanding the drivers, intentions, and motives of

foreign actors and the history, context, and personalities shaping their actions is primarily the realm of human experts. As AI technology advances, it may grow more able to determine these drivers and thus help predict and project *the outlook* of where an issue is heading. Explaining *the implications* of intelligence for U.S. policymakers will remain the unique strength of the human analyst.

While emerging technology will provide immense value to IC analysis, another question will emerge in the years ahead: what is the value of IC analysis itself to U.S. policy? While the IC will still enjoy many advantages, namely in classified collection, the combination of high-quality OSINT, commercially available GEOINT and SIGINT, and data analytics will level the analytic playing field. Any trained and equipped organization will be able to generate all-source analysis of current events of comparable quality to IC analysts—at a faster pace and a fraction of the cost. In future information environments of ubiquitous sensing and continual awareness, the commercial sector's faster technology adoption rates and superior facility with OSINT could give it the advantage over the IC in assessing *what* is happening in fast-moving global events.

IC analysts will likely have a diminished competitive advantage in delivering current intelligence to U.S. policymakers on current threats and events in the years ahead. But, to paraphrase another intelligence question, *so what?* As the IC aims to distinguish itself from open source, its value to U.S. policy will not stem from being a slightly better "classified CNN" analyzing current events. While the IC can and must deliver timely analysis to remain relevant to policymakers, the strength of the IC will remain the experience and expertise of its seasoned analysts and what they alone can provide policymakers: unique and unrivaled insight into the *why*, the *outlook*, and the *implications* of global events and emerging threats for U.S. interests.

Emerging technologies, of course, will still be vital. An IC analyst armed with the AI and OSINT to make rapid sense of *what* is happening and clandestine intelligence and historic context to know *why* will be able to provide unmatched insight on global threats, future scenarios, and the implications for U.S. policy. The combination of emerging technologies, human subject matter expertise, and IC tradecraft will leave IC analysts uniquely positioned to answer the types of vexing and often technologically oriented questions policymakers will pose in the coming years.

- **What's *new?*** As U.S. competitors increasingly adopt irregular, indirect, and clandestine approaches short of war to gain strategic advantage, analysts must be able to detect new and incremental "gray zone" activity in the political, paramilitary, information, and economic realms.[45] Analysts with AI-enabled signal detection, pattern finding, and visualization tools and expertise on adversary strategy, operations, and doctrine will be best positioned to spot new operations, discern incremental but meaningful change in operational environments, provide early warning to U.S. decisionmakers, and mitigate risk of strategic surprise.
- **What's *true?*** As foreign disinformation and influence campaigns accelerate—with greater speed, scale, sophistication, and seeming authenticity—policymakers will turn to the IC to help separate "truth from fiction." Analysts will need AI capabilities such as in generative adversarial networks to detect synthetic and inauthentic deepfakes and sentiment analysis to measure influence operations' impact. Analysts with baseline technical skills and country expertise will be ideally suited to assess adversaries' information warfare strategy and potential future operations.
- **What's *next?*** Anticipatory strategic intelligence is less about predicting specific threats than envisioning and correctly assessing the likelihood of potential events and adversary actions. AI-enabled modeling, war gaming, and scenarios analysis could help analysts to discern and discover potential courses of action, predict adversary decision points, and identify signposts of low probability-high impact scenarios for U.S. interests before they occur
- An IC analyst armed with the AI and OSINT to make rapid sense of *what* is happening and clandestine intelligence and historic context to know *why* will be able to provide unmatched insight on global threats, future scenarios, and the implications for U.S. policy.

An IC analyst armed with the AI and OSINT to make rapid sense of what is happening and clandestine intelligence and historic context to know why will be able to provide unmatched insight on global threats, future scenarios, and the implications for U.S. policy.

IMPLICATIONS: EMPOWERING THE ANALYST OF TODAY AND TOMORROW

The IC's ability to integrate and leverage innovative technology for strategic analysis will be vital in generating and sustaining policymakers' decisionmaking advantage over increasingly sophisticated adversaries and rivals. To maintain the analytic edge, the IC must simultaneously begin envisioning, planning, and resourcing the analytic missions of the future while rapidly embracing and assimilating emerging technologies into present-day tradecraft.

Bridging the continuum from current to future analytic needs will be the analysts themselves. With limited hiring, long lead times, small turnover, and high retention, the IC workforce cannot be easily refreshed and transformed with new technologically-savvy talent.[46] Indeed, "the workforce of the future," as former CIA chief learning officer Joseph Gartin asserts, "is already here," and the analysts of 2020 will be the leaders, managers, and, for many, still analysts of 2030. IC leaders and critical stakeholders—policymakers, Congress, and the technology and research sectors—must provide the analytic workforce the technology and training to thrive today while laying the digital groundwork, institutional priorities, and cultural norms for future success. How?

- **Embracing OSINT**: The IC must reconceptualize OSINT as a foundational INT alongside traditional clandestine intelligence collection in informing and driving analytic judgments and a strategic necessity in a world of big data. Moreover, OSINT could serve as not only a vital input to classified assessments but also as an analytic mission in its own right. The combination of high-quality OSINT and commercial GEOINT and SIGINT means that all-source intelligence analysis can now be crafted at the unclassified level. Instead of viewing it as competition, the IC could embrace "finished OSINT" as an opportunity to expand its reach and impact to new customers and stakeholders likely to value IC tradecraft and insight but at the unclassified level, including domestic law enforcement, foreign governments, the technology and industrial sectors, and the broader U.S. public.
- **Elevating TECHINT**: Intelligence of foreign AI systems and S&T capabilities, plans, and intentions must also be conceived as a foundational intelligence mission, spanning collection and analysis and essential for planning and resourcing future IC missions. The IC should be able to understand and forecast emerging technologies—particularly AI, biotechnology, and quantum computing—and their applications for foreign statecraft, economic competitiveness, and military and intelligence operations. Doing so will require both clandestine collection of adversary technological capabilities and applications and well-sourced OSINT of foreign S&T sector innovation, including patents, partnerships, acquisitions, and expansion. Analysts will need more technical and tactical knowledge to understand foreign AI systems as well as the capabilities and limitations of their own AI-enabled collection, targeting, and acquired data.
- **Integrating Technologists:** Analysts will need to develop some level of digital acumen in data science and AI, but collaboration and teaming with true technologists—data scientists, ML engineers, and product designers—could unlock AI's true potential for analysis. Integrating data scientists into analytic units will help data scientists understand the analytic problem set and analysts comprehend the underlying AI, enabling partnering to hone and tailor models, apply the right tools to the right datasets, and attribute meaning to results.[47] ML engineers and product designers will need access to the analyst end user to understand how to design, build, and adapt software, tools, and interfaces suited to analysts' unique needs and requirements.
- **Proliferating Pockets of Success**: While creating the digital infrastructure and institutional incentives for enterprise-wide technological adoption, IC leaders should empower individual directorates and mission centers to acquire, experiment with, and adopt the tools that fit their unique mission needs. Certain analytic missions, particularly more operational intelligence-focused ones such as CT, will be better suited to harness AI/ML. But IC leaders should identify the attributes, norms, and best practices of units embracing tech transformation and seek to proliferate the lessons learned to spur creative approaches across organizations.

The IC must reconceptualize OSINT as a foundational INT alongside traditional clandestine intelligence collection in informing and driving analytic judgments and a strategic necessity in a world of big data.

- **Educating Policymakers**: Analytic value ultimately derives from a product's impact on policy customers and their trust in its analytic quality, clarity, and transparency in explaining its judgments. As the IC moves to integrate AI and data analytics into its products, analysts must be able to clearly and convincingly explain to policymakers how these technologies were applied, their relative weight in forming assessments, and their impact on confidence levels of key judgments. Analysts will need to become educators on AI and analytics applications and learn to build trust with the strategic leaders making critical policy and operational decisions based on their AI-enabled analysis.

The IC must reconceptualize OSINT as a foundational INT alongside traditional clandestine intelligence collection in informing and driving analytic judgments and a strategic necessity in a world of big data.

The IC's embrace of emerging technologies could enable an even closer relationship between analysts and customers and help facilitate such enhanced analyst-policymaker interaction, which we will explore in phase three of the Task Force, focused on intelligence *distribution.* ■

Brian Katz *is a fellow in the International Security Program at the Center for Strategic and International Studies (CSIS) and research director of the CSIS Technology and Intelligence Task Force.*

This report is made possible by support to the CSIS Technology and Intelligence Task Force from Booz Allen Hamilton, Rebellion Defense, Redhorse, and TRSS.

ENDNOTES

1 Two definitions of AI are useful for this report. First, AI is "the ability of a computer system to solve problems and to perform tasks that would otherwise require human intelligence." See National Security Commission on Artificial Intelligence (NSCAI), Interim Report (Arlington, VA: NSCAI, 2019). Second, AI is "systems that extend human capability by sensing, comprehending, acting, and learning." See Dougherty and Wilson, Human + Machine.

2 "The field of study interested in building computational systems that can improve their own performance of some task." See ODNI, The AIM Initiative.

3 "A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services)." See ODNI, Strategic Plan to Advance Cloud Computing in the Intelligence Community (Washington, D.C.: ODNI, 2019).

4 Office of the Director of National Intelligence (ODNI), The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines (Washington, DC: ODNI, 2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf.

5 U.S. government official remarks at CSIS Technology and Intelligence Task Force meeting, July 2020.

6 Ibid.

7 U.S. software and analytics firm research interview, interview by CSIS Intelligence and Technology Task Force, July 2020.

8 U.S. defense and technology firm research interview, interview by CSIS Intelligence and Technology Task Force, June 2020.

9 U.S. technology and cloud-computing services firm research interview, interview by CSIS Intelligence and Technology Task Force, June 2020.

10 "A field of study that aims to analyze and understand human language communications both spoken and textual. Can include analysis and generation of language." See ODNI, The AIM Initiative.

11 Brian Raymond, "How Emerging AI Technologies Can Help US Think 'Smarter,'" Primer AI (blog), March 21, 2019, https://primer.ai/blog/how-emerging-ai-technologies-can-help-us-think-smarter/.

12 Ibid.

13 U.S. defense and technology firm research interview.

14 U.S. technology and cloud-computing services firm research interview.

15 Ibid.

16 Raymond, "How Emerging AI Technologies.'"

17 U.S. machine intelligence firm research interview, interview by CSIS Intelligence and Technology Task Force, July 2020.

18 Ibid.

19 Raymond, "How Emerging AI Technologies."

20 Ibid.

21 "A statistical technique that exploits large quantities of data as training sets for a network with multiple hidden layers, called a deep neural network (DNN). A DNN is trained on a data set, generating outputs, calculating errors, and adjusting its internal parameters . . . It has proved to be an effective technique for image classification, object detection, speech recognition, and natural language processing." See National Security Commission on Artificial Intelligence, Interim Report.

22 U.S. technology and cloud-computing services firm research interview.

23 U.S. technology and analytics firm research interview, interview by CSIS Intelligence and Technology Task Force, June 2020.

24 U.S. data science and analytics firm research interview, interview by CSIS Intelligence and Technology Task Force, June 2020.

25 U.S. machine intelligence firm research interview, interview by CSIS Intelligence and Technology Task Force, July 2020.

26 Ibid.

27 U.S defense and technology firm research interview.

28 Paul J. H. Schoemaker and Philip E. Tetlock. "Superforecasting: How to Upgrade Your Company's Judgment," Harvard Business Review, May 2016, https://hbr.org/2016/05/superforecasting-how-to-upgrade-your-companys-judgment.

29 ODNI, The AIM Initiative.

30 Joichi Ito, "Forget about artificial intelligence, extended intelligence is the future," MIT Media Lab, April 24, 2019, https://www.media.mit.edu/articles/forget-about-artificial-intelligence-extended-intelligence-is-the-future/.

31 Raymond, "How Emerging AI Technologies."

32 Joseph W. Gartin, "The Future of Analysis," Studies in Intelligence 63, no. 2 (June 2019).

33 U.S. technology and cloud-provider firm research interview, interview by CSIS Intelligence and Technology Task Force, June 2020.

34 Ibid.

35 U.S. government official remarks at CSIS Technology and Intelligence Task Force meeting, July 2020.

36 U.S. technology and cloud-provider firm research interview.

37 U.S. technology and analytics firm research interview.

38 Paul R. Dougherty and H. James Wilson, Human + Machine: Reimagining Work in the Age of AI (Cambridge, MA: Harvard Business Review Press, 2018),

39 Joseph Gartin, "Thinking About the IC's Talent Management Issues in an AI/ML Environment," Elevated Debate, July 8, 2020, https://elevateddebate.com/thinking-about-the-ics-talent-management-issues-in-an-ai-ml-environment/.

40 Congressional Research Service, Artificial Intelligence and National Security (Washington, D.C.: CRS); Patrick Tucker, "What the CIA's Tech Director Wants from AI," Defense One, September 6, 2017, https://www.defenseone.com/technology/2017/09/cia-technology-director-artificial-intelligence/140801/.

41 "Two neural networks are trained in tandem: one is designed to be a generative network (the forger) and the other a discriminative network (the forgery detector). The objective is for each to train and better itself off the other, reducing the need for big labeled training data." See National Security Commission on Artificial Intelligence, Interim Report.

42 ODNI, The AIM Initiative; CRS, Artificial Intelligence and National Security; Erik Lin-Greenberg, "Allies and Artificial Intelligence," Texas National Security Review 3, no. 2 (Spring 2020): 56-76.

43 U.S. AI security software and analytics firm research interview, interview by CSIS Intelligence and Technology Task Force, July 2020.

44 Ibid.

45 For more analysis on competition in the "gray zone," see the CSIS Gray Zone Project at https://www.csis.org/grayzone.

46 Gartin, "Thinking About the IC's Talent Management Issues."

47 U.S. technology and analytics firm research interview.