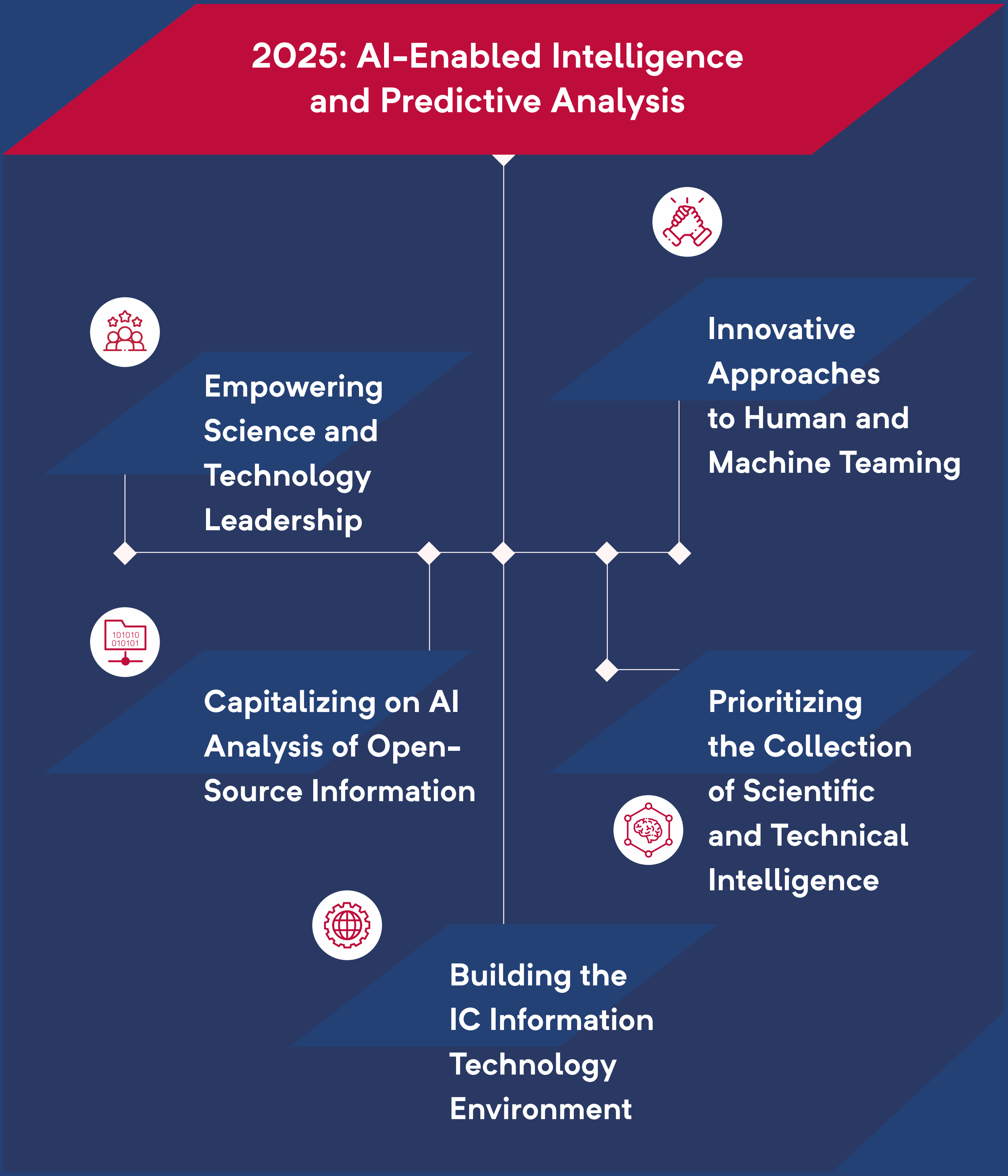
Chapter 5: AI and the Future of National Intelligence



2025: AI-Enabled Intelligence and Predictive Analysis

Empowering Science and Technology Leadership

Innovative Approaches to Human and Machine Teaming

Capitalizing on AI Analysis of Open-Source Information

Prioritizing the Collection of Scientific and Technical Intelligence

Building the IC Information Technology Environment

Intelligence will benefit from rapid adoption of artificial intelligence (AI)-enabled technologies more than any other national security mission. As every possible platform—both machine and human—contributes to the global information grid, and as the number of sensors grows exponentially, the volume, velocity, and variety of data threaten to overwhelm intelligence analysis. Ascertaining the veracity and value of information will be harder. Analysts will be challenged to provide the context crucial for turning information into actionable intelligence.

AI will help intelligence professionals find needles in haystacks, connect the dots, and disrupt dangerous plots by discerning trends and discovering previously hidden or masked indications and warnings. AI-enabled capabilities will improve every stage of the intelligence cycle from tasking through collection, processing, exploitation, analysis, and dissemination. AI algorithms can sift through vast amounts of data to find patterns, detect threats, identify correlations, and make predictions. AI tools can make satellite imagery, communications signals, economic indicators, social media data, and other large sources of information more intelligible. AI can find correlations between open-source data and other sources of intelligence, and help the Intelligence Community (IC) be more precise, efficient, and effective in its targeting and collections activities. The constellation of current and emerging AI technologies applicable to intelligence missions includes computer vision for imagery analysis, biometric technologies (such as face, voice, and gait recognition), natural language processing, and algorithmic search and query functions for large databases, among others. Most important, AI enables data fusion from dissimilar data streams to create a composite picture.[1]

In military scenarios—against technologically advanced adversaries, rogue states, or terrorist organizations—AI-enabled intelligence, surveillance, and reconnaissance platforms and AI-enabled indication and warning (I&W) systems will be critical for the kind of advanced warfighting capabilities discussed in Chapter 3 of this report. Through automation, AI-enabled systems will optimize tasking and collection for platforms, sensors, and assets in near-real time in response to dynamic intelligence requirements or changes in the environment. At the tactical edge, "smart" sensors will be capable of pre-processing raw intelligence and prioritizing the data to transmit and store, which will be especially helpful in degraded or low-bandwidth environments. Once collected, intelligent processing systems can triage the information, identify trends and patterns, summarize key implications, and prepare the highest-priority information for human review (or flag items of particular interest, based on analyst-defined conditions). This includes advanced I&W systems that will enable warfighters to anticipate and understand emerging threats earlier, allowing them to proactively shape the environment, as well as systems close to the tactical edge identifying adversarial denial and deception efforts. When paired with human judgment, these capabilities will enhance all-domain awareness, lead to tighter and more informed decision cycles, offer recommendations for different courses of action, and allow rapid counter-actions to adversary actions.

The need to adapt is made urgent by the quickening diffusion of these new technologies. Once exquisite IC capabilities are now in wide use around the world.[2] Our adversaries' ability to quickly adopt AI tools means that the IC may be more vulnerable to deception, information operations, sources and methods exposure, cyber operations, and counterintelligence activities. The IC has been an early mover within the government in establishing some of the underlying infrastructure to enable the adoption of AI, such as contracting an IC-wide commercial cloud service in 2013.[3] In addition, the IC's 2019 Augmenting Intelligence using Machines (AIM) initiative provided direction and a framework for broader adoption, and some intelligence agencies have made great strides in AI adoption, putting them ahead of others in government. Still, critical barriers in authorities, policies, budgets, data sharing, and technical standards keep the IC from fully realizing its potential, and none of these recommendations will be effective without substantial reforms of the security clearance process.

An Ambitious Agenda: AI-Ready by 2025.

To build on the progress that individual agencies have made, the IC should set the ambitious goal of adopting and integrating AI-enabled capabilities across every possible aspect of the intelligence enterprise as part of a larger vision for the future of intelligence.

An AI-Ready IC by 2025:

Intelligence professionals enabled with baseline digital literacy and access to the digital infrastructure and software required for ubiquitous AI integration in each stage of the intelligence cycle.

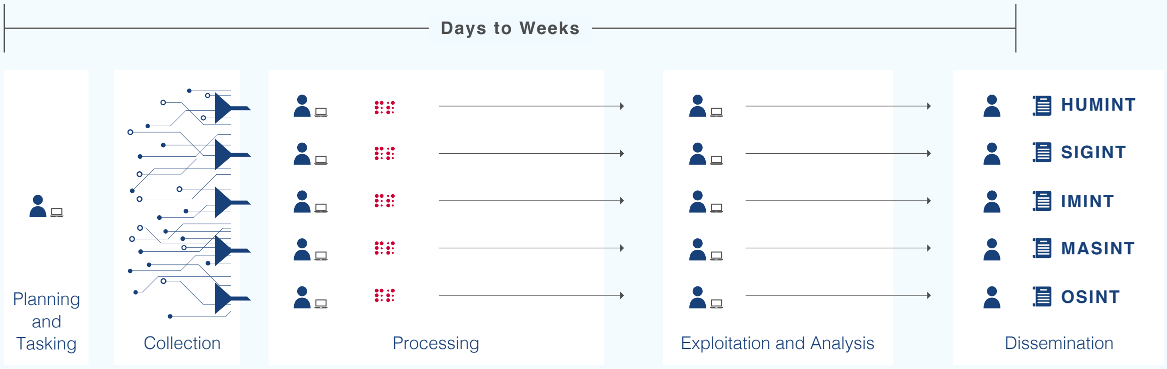
Starting immediately, the IC should prioritize automating each stage of the intelligence cycle to the greatest extent possible and processing all available data and information through AI-enabled analytic systems before human analyst review. Products should also be disseminated at machine speed–which means they must be in machine-readable formats–and systems across the IC must be able to ingest and use them without manual intervention. Optimizing AI-enabled systems in this way will require an entirely different approach to the creation and review of finished intelligence products. The IC should require that all intelligence products include both a human-readable version and, just as important, an automated machine-readable version that can be ingested into other analytic systems throughout the IC. All future intelligence systems should be optimized for AI-oriented data collection and processing.

"The IC should require that all intelligence products include both a human-readable version and, as importantly, an automated machine-readable version that can be ingested into other analytic systems throughout the IC."

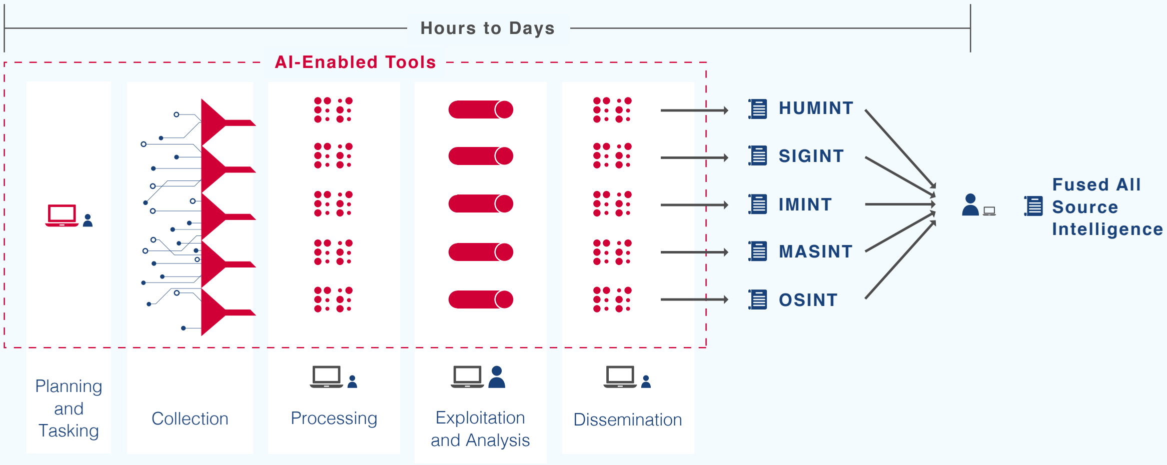
Once the IC has automated its processes within individual intelligence disciplines, it should fuse those individual processes into a continuous pipeline of all-source intelligence analysis processed through a federated architecture of continually learning analytic engines. This transformational change could lead to insights arising from human-machine teaming that are beyond the current limits of unaided human cognition. Such a system would bring greater clarity to ongoing developments and also enable more accurate and reliable predictive analysis of emerging threats. As analysts gain more trust in AI-enabled systems, the ratio of human- to machine-led analysis will tip more heavily toward machines.

AI-Enabled National Intelligence.

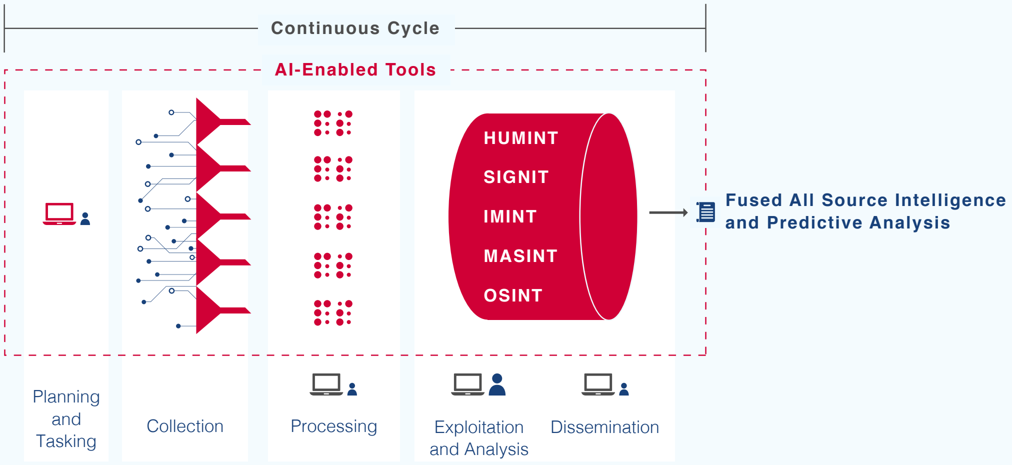
Current



Optimized: AI-Enabled Automation within Current Intelligence Disciplines



Transformed: AI-Enabled All Source Intelligence and Predictive Analysis



Preparing for an AI-ready 2025 demands the following actions:

Recommendation

Empower the IC's science and technology leadership. The Director of National Intelligence (DNI) should designate the Director of Science and Technology (S&T) within the Office of the Director of National Intelligence (ODNI) as the IC's Chief Technology Officer (CTO) and task and empower this position to drive the IC's adoption of AI-enabled applications to solve operational intelligence requirements. To do so, the IC CTO should oversee the AIM strategy, establish and enforce common technical standards and policies necessary to rapidly and responsibly scale AI-enabled applications across the IC, and lead acquisition reform to ensure that the IC can rapidly procure and field systems to its intelligence professionals. The IC CTO should be granted additional authorities for establishing policies on and supervising IC research and engineering, technology development, technology transition, appropriate prototyping activities, experimentation, and developmental testing activities.

Recommendation

Change risk management practices to accelerate new technology adoption. The IC needs to balance the technical risks involved in bringing new technologies online and quickly updating them with the substantial operational risks that result from not keeping pace, similar to DoD. Regular software upgrades should be automated to the extent possible. To share software tools more easily among agencies, reciprocal accreditation of information technology systems should be the standard.[4]

> **"The IC needs to balance the technical risks involved in bringing new technologies on line and quickly updating them with the substantial operational risks that result from not keeping pace ..."**

To coordinate these changes, the ODNI should establish a Senior Risk Management Council focused on technology modernization.[5] Its task should be to weigh the risks of adopting new technologies with the opportunity costs of not doing so. Its goal should be to ensure that analysts have access to the tools they need to do their jobs.

The IC will need support from the intelligence committees in Congress––for example, in the flexible use of funds within a more agile software development framework. To support the argument for greater flexibility, the IC should develop data-driven ways of communicating operational gains, as well as credible assessments of the risk of inaction.

Recommendation

Improve coordination and interoperability between the IC and DoD. The IC must aggressively pursue automated interoperability with the DoD for intelligence operations conducted at machine speeds.[6] To do this, security managers and network administrators must build greater confidence in fast and secure data exchanges. ODNI, the Under Secretary of Defense for Intelligence and Security, and the Joint Artificial Intelligence Center (JAIC) should coordinate more on intelligence-related AI projects to minimize duplication of effort while maximizing common approaches to AI capability development, testing and evaluation, deployment, international engagement, and policies and authorities. They should work together to create interoperable and sharable resources and tools––such as those envisioned in the AI R&D ecosystem described in Chapter 2 of this report––and should establish a culture of sharing all AI-enabled capabilities whenever feasible.[7]

Recommendation

Capitalize on AI-enabled analysis of open-source and publicly available information.[8] The IC should develop a coordinated and federated approach to applying AI-enabled applications to open-source intelligence (OSINT) and should strive to integrate open-source analysis into existing intelligence processes wherever possible in every intelligence domain.[9]

Recommendation

Prioritize and accelerate collection of scientific and technical intelligence to better understand adversary capabilities and intentions. Such collection requires the IC to significantly increase the technical sophistication, capabilities, and capacity of its analytic workforce. That must involve aggressive efforts to train, recruit, and retain analysts who have the requisite skills. These analysts must guide collection requirements and provide timely, accurate assessments. To better coordinate intelligence on these topics, including collecting on scientific and technical cooperation among our competitors, the DNI should appoint an Emerging Technology Collection Executive within the National Intelligence Council.[10]

Recommendation

To recruit more S&T experts into the IC, aggressively pursue security clearance reform for clearances at the Top Secret level and above, and enforce security clearance reciprocity among members of the IC. ODNI should develop and implement an AI-enabled data and science-based approach to security-clearance adjudication that significantly shortens investigation timelines.[11]

Recommendation

Advance and continue to develop a purpose-built IC Information Technology Environment that can fuse intelligence from different domains and sources. An AI-enabled technical architecture of this kind could help autonomously integrate intelligence across stove-piped intelligence domains, which currently often require manual intervention to share raw data or finished analysis.[12] Doing so would help the IC blend insights from different streams of information to create a composite picture. For example, signals intelligence often depends upon human intelligence or geospatial intelligence. Likewise, the value of human intelligence can almost always be enhanced by layering signals intelligence or open-source information on top of it.

Recommendation

Embrace fused, predictive analysis as the new standard. Successfully fusing all-source/all-domain intelligence will enable accurate predictive analysis in a way that is not currently possible. The government's response to the COVID-19 virus has offered glimpses into the potential for fused data sets to inform such analysis. For example, U.S. Northern Command (working with the JAIC and the National Guard Bureau) built predictive models from dozens of different data sets that helped to identify COVID-19 hotspots and reconcile demands for critical supplies.[13]

Recommendation

Develop innovative human-centric approaches to human-machine teaming. The kind of data fusion envisioned here through autonomous machine-to-machine integration will require new concepts for human-machine teaming that optimize the strengths of each.[14] The IC will need new approaches that amplify and extend human cognition to effectively handle the scale and complexity of the information generated by all-source intelligence analytic engines. When developing these systems, the IC must understand and make deliberate decisions on when and under what conditions the human or machine should act alone and under what conditions human-machine teaming is desirable.

"The kind of data fusion envisioned here through autonomous machine-to-machine integration will require new concepts for human-machine teaming that optimize the strengths of each."

Chapter 5 - Endnotes

[1] For additional information on AI-enabled use cases throughout the intelligence cycle, see the discussion on “Applications” in *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence Through Innovation*, CSIS Technology and Intelligence Task Force at 8-22 (Jan. 13, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

[2] *AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*, Office of the Director of National Intelligence (2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf (foreword by the Honorable Sue Gordon, Principal Deputy Director of National Intelligence).

[3] Frank Konkel, *The Details about the CIA’s Deal with Amazon*, The Atlantic (July 14, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/.

[4] In adopting new software systems, the IC follows a risk-management framework developed by the National Institute of Standards and Technology (NIST). While it is a useful framework overall, it can also create delays or prevent the IC from keeping up with cutting-edge AI tools that are commercially available. For more information, see *FISMA Implementation Project*, NIST (Dec. 3, 2020), https://csrc.nist.gov/projects/risk-management/rmf-overview.

[5] The Senior Risk Management Council would help the IC implement guidance from the proposed Tri-Chair Committee on Emerging Technology and function similarly to the role this commission recommended for the Under Secretary of Defense for Research and Engineering as a co-chair on the Joint Requirements Oversight Council in DoD.

[6] For more information, see Kent Linnebur, et al., *Intelligence After Next: The Future of the IC Workplace*, MITRE Center for Technology and National Security (Nov. 1, 2020), https://www.mitre.org/sites/default/files/publications/pr-20-1891-intelligence-after-next-the-future-of-the-ic-workplace.pdf.

[7] These efforts should leverage the JAIC’s Joint Common Foundation (JCF).

[8] Pub. L. 116-260, The Consolidated Appropriations Act (2021), Division W, Section 326 (“Open source intelligence strategies and plans for the intelligence community”), Section 623 (“Independent study on open-source intelligence”), and Section 624 (“Survey on Open Source Enterprise”) provide a starting point for the IC to reimagine the role of open-source intelligence.

[9] It is important to note that open-source intelligence (OSINT) is not limited to traditional media sources (newspapers, radio broadcasts, etc.) and social media. OSINT also includes publicly available information such as public government data sources (official reports, budget documents, hearing testimonies, etc.), professional and academic publications, commercial data sources (industry reports, financial statements, commercial imagery, etc.), and more.

[10] For additional information, see the discussion on “Elevating Technical Intelligence” in *Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence Through Innovation*, CSIS Technology and Intelligence Task Force at 12 (Jan. 13, 2021), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210113_Intelligence_Edge.pdf.

[11] For more information on the need for an academic and scientific review of behavioral approaches to security clearance adjudication, see David Luckey, et al., *Assessing Continuous Evaluation Approaches for Insider Threats: How Can the Security Posture of the U.S. Departments and Agencies Be Improved?*, RAND Corporation at 28-34 (2019), https://www.rand.org/pubs/research_reports/RR2684.html.

Chapter 5 - Endnotes

[12] The technical aspects of such an environment are covered in more detail in Chapter 2 of this report.

[13] Air Force General Terrence J. O'Shaughnessy, Commander, U.S. Northern Command & Army Lieutenant General Laura J. Richardson, Commander, U.S. Army North, *Transcript: US NORTHCOM and ARNORTH Commanders Discuss Ongoing COVID-19 Efforts*, U.S. Department of Defense (April 21, 2020), https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/2160070/us-northcom-and-arnorth-commanders-discuss-ongoing-covid-19-efforts/.

[14] See Kenneth M. Ford, et al., *Cognitive Orthoses: Toward Human-Centered AI*, AI Magazine at 7 (Winter 2015), https://doi.org/10.1609/aimag.v36i4.2629; John Laird, et al., *Future Directions in Human Machine Teaming Workshop*, U.S. Department of Defense (July 16-17, 2019), https://basicresearch.defense.gov/Portals/61/Future%20Directions%20in%20Human%20Machine%20Teaming%20Workshop%20report%20%20%28for%20public%20release%29.pdf; Gagan Bansal, et al., *Is the Most Accurate AI the Best Teammate? Optimizing AI for Teamwork*, AAAI 2021 (Feb. 2021), https://www.microsoft.com/en-us/research/publication/is-the-most-accurate-ai-the-best-teammate-optimizing-ai-for-teamwork/.