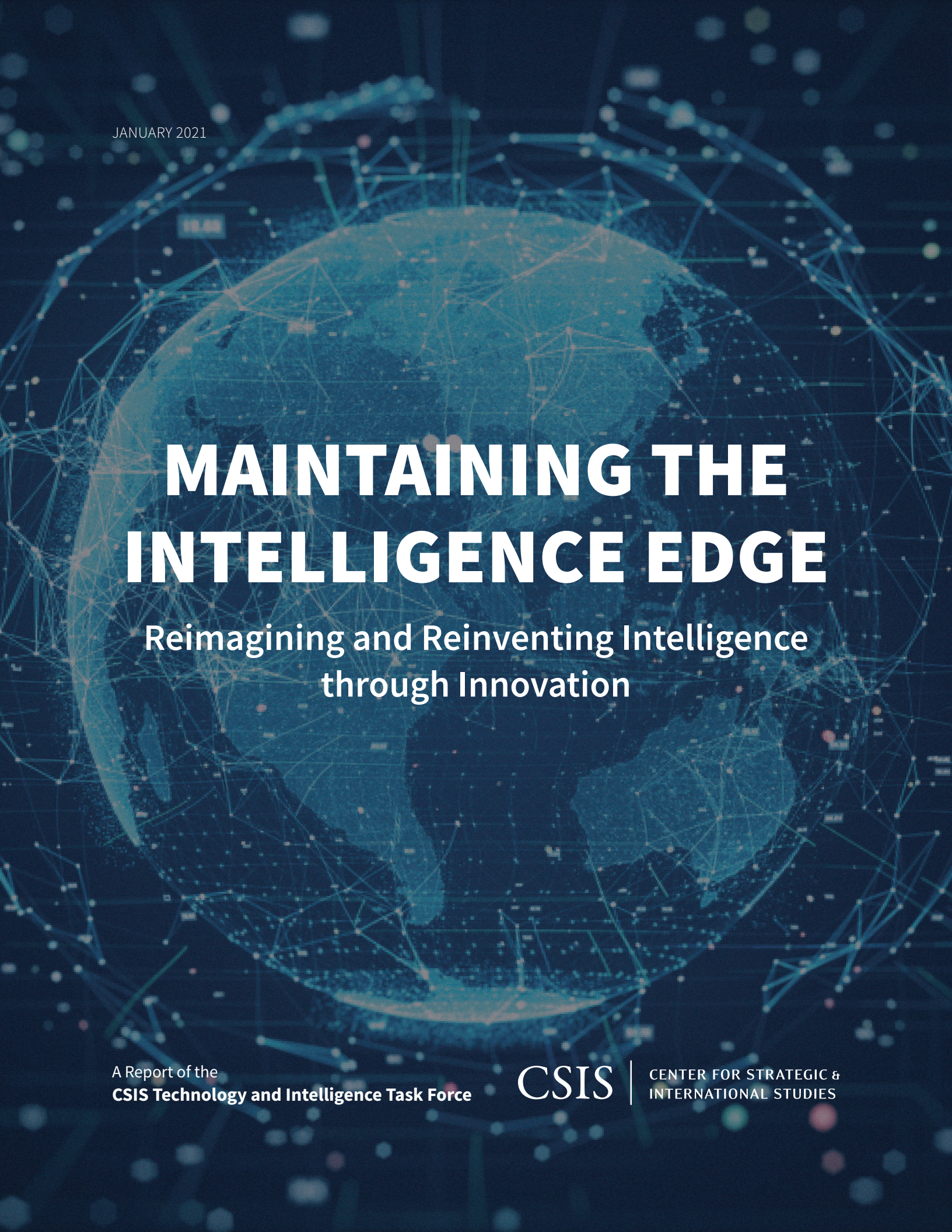


JANUARY 2021

MAINTAINING THE INTELLIGENCE EDGE

Reimagining and Reinventing Intelligence through Innovation

A Report of the
CSIS Technology and Intelligence Task Force

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

JANUARY 2021

MAINTAINING THE INTELLIGENCE EDGE

Reimagining and Reinventing Intelligence through Innovation

A Report of the
CSIS Technology and Intelligence Task Force

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

ABOUT CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. Senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS is ranked the number one think tank in the United States as well as the defense and national security center of excellence for 2016-2018 by the University of Pennsylvania's "Global Go To Think Tank Index."

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2021 by the Center for Strategic and International Studies.
All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

CSIS TECHNOLOGY AND INTELLIGENCE TASK FORCE

Co-Chairs

Avril Haines*
Former Deputy National Security Advisor and Deputy Director of the Central Intelligence Agency

Stephanie O'Sullivan
Former Principal Deputy Director for National Intelligence

Commissioners

Michael Allen
Managing Director of Beacon Global Strategies LLC; Former Majority Staff Director of the House Permanent Select Committee on Intelligence

Kari Bingen
Former Deputy Under Secretary of Defense for Intelligence and Security

Robert Cardillo
President, The Cardillo Group;
Former Director of the National Geospatial-Intelligence Agency

John P. Carlin
Partner, Morrison & Foerster;
Former Assistant Attorney General for National Security

Rick Ledgett
Senior Advisor at Hakluyt Cyber;
Former Deputy Director of the National Security Agency

Marcel Lettre
Former Under Secretary of Defense for Intelligence

Jason Matheny
Founding Director of Georgetown's Center for Security and Emerging Technology; Former Assistant Director of National Intelligence and Director of the Intelligence Advanced Research Projects Activity

John McLaughlin
Distinguished Practitioner in Residence, The Johns Hopkins University School of Advanced International Studies; Former Deputy Director and Acting Director of the Central Intelligence Agency

Jami Miscik
CEO of Kissinger Associates, Inc.;
Former Deputy Director for Intelligence at the Central Intelligence Agency

---

* Avril Haines stepped down from her role as co-chair and left the task force at the end of July 2020.

Stephen Slick
Director of The University of Texas at Austin's Intelligence Studies Project; Former CIA Clandestine Service Officer and National Security Council Senior Director for Intelligence Programs and Reform

Gen. Joseph L. Votel
USA (Ret.), President and CEO of Business Executives for National Security; Former Commander of U.S. Central Command and U.S. Special Operations Command

Amy Zegart
Senior Fellow at the Freeman Spogli Institute of International Studies and Davies Family Senior Fellow at the Hoover Institution, Stanford University

CSIS Experts

Kathleen Hicks, Task Force Senior Adviser
Former Senior Vice President, Henry A. Kissinger Chair, and Director of the International Security Program, CSIS

Brian Katz, Task Force Research Director
Fellow, International Security Program, CSIS

Previous Task Force Reports

Brian Katz, "The Intelligence Edge: Opportunities and Challenges from Emerging Technologies for U.S. Intelligence," CSIS, *CSIS Brief*, April 17, 2020, https://www.csis.org/analysis/intelligence-edge-opportunities-and-challenges-emerging-technologies-us-intelligence.

Brian Katz, "The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection," CSIS, *CSIS Brief*, July 13, 2020, https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

Brian Katz, "The Analytic Edge: Leveraging Emerging Technologies to Transform Intelligence Analysis," CSIS, *CSIS Brief*, October 9, 2020, https://www.csis.org/analysis/analytic-edge-leveraging-emerging-technologies-transform-intelligence-analysis.

ACKNOWLEDGMENTS

The CSIS Technology and Intelligence Task Force is indebted to the dozens of intelligence, innovation, and policy leaders and experts who generously contributed their time, insights, and effort to the task force. First and foremost, the task force relied upon the leadership of its co-chairs and the dedication of its 12 commissioners, whose mix of intelligence and national security, technology, and academic experience was essential in driving and informing this ambitious yearlong endeavor.

A central finding of the task force is that reinvention of the Intelligence Community (IC) through innovation will require the buy-in, support, and dedication of a variety stakeholders—in the IC, Congress, defense, technology, and research sectors. Over the course of the past year, the task force received just such commitment and passion from leaders and experts across these communities through several dozen "deep-dive" briefings.

In the IC, the Office of the Director of National Intelligence (ODNI) provided critical guidance and insights throughout the year for our research efforts, as well as laying the groundwork for intelligence innovation and this study with its Augmenting Intelligence Using Machines (AIM) Initiative. An array of senior leaders and experts at the Central Intelligence Agency, Defense Intelligence Agency, and National Geospatial-Intelligence Agency also provided key ideas and insights.

The task force benefited from multiple engagements with the various and thriving innovation and research centers across the IC and U.S. Department of Defense (DOD), including the Defense Advanced Research Projects Activity (DARPA), Intelligence Advanced Research Projects Activity (IARPA), In-Q-Tel, and DOD Joint Artificial Intelligence Center (JAIC).

The IC is not lacking for cutting-edge U.S. technology and innovation firms willing to support the IC mission. More than a dozen firms provided critical tech deep-dives to the task force, including: Anduril, Amazon Web Services, CalypsoAI, Ginkgo Bioworks, Google, Microsoft, Palantir, and Primer AI.

The task force received invaluable support from the professional staff of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence, whose own dedication to and work on these issues will be essential for intelligence innovation.[1]

The task force research effort benefitted from and relied upon the sterling work of colleagues also exploring intelligence innovation, including the National Security Commission on AI, the Intelligence National Security Alliance, and other research institutes.

Finally, the task force itself would not have been possible without the generous support its four sponsoring organizations—Booz Allen Hamilton, Rebellion Defense, Redhorse, and TRSS.

CONTENTS

ABBREVIATIONS AND ACRONYMS

5G – fifth-generation telecommunications technology

AI – artificial intelligence

API – application programming interface

C2S – Commercial Cloud Services

CI – counterintelligence

CIA – Central Intelligence Agency

CT – counterterrorism

CTO – chief technology officer

DARPA – Defense Advanced Research Projects Agency

DEI – diversity, equity, and inclusion

DevSecOps – development, security, and operations

DIA – Defense Intelligence Agency

DNI – Director of National Intelligence

DO – CIA Directorate of Operations

DOD – Department of Defense

FVEY – Five Eyes intelligence alliance

GAN – generative adversarial network

GEOINT – geospatial intelligence

GPU – graphics processing unit

HPSCI – House Permanent Select Committee on Intelligence

HUMINT – human intelligence

IARPA – Intelligence Advanced Research Projects Activity

IC – U.S. Intelligence Community

IC ITE – Intelligence Community Information Technology Enterprise

IIB – Intelligence Innovation Board

IoT – Internet of Things

JAIC – Joint Artificial Intelligence Center

ML – machine learning

NIC – National Intelligence Council

NLP – natural language processing

ODNI – Office of the Director of National Intelligence

OSINT – open-source intelligence

NGA – National Geospatial-Intelligence Agency

NIPF – National Intelligence Priorities Framework

NSA – National Security Agency

NSC – National Security Council

OSC – Open Source Center

OSIA – Open Source Intelligence Agency

PAI – publicly available information

PDB – President's Daily Brief

PDD – Presidential Decision Directive

PDDNI – Principal Deputy Director of National Intelligence

S&T – science and technology

SIGINT – signals intelligence

T&E – testing and evaluation

TEVV – testing, evaluation, verification, and validation

TCPED – tasking, collection, processing, exploitation/analysis, and dissemination

TECHINT – technical intelligence

TS/SCI – Top Secret/Sensitive Compartmented Information

UI/UX – user interface/user experience

USDI&S – Undersecretary of Defense for Intelligence and Security

VR/AR – virtual reality/augmented reality

EXECUTIVE SUMMARY

The U.S. Intelligence Community (IC) stands at the dawn of a new era of technological innovation and transformation unprecedented in its history. Driven by artificial intelligence (AI) and associated emerging technologies, including cloud computing, advanced sensors, and big data analytics, the approaching "AI era" will transform both the nature of the global threats the IC is responsible for assessing and the IC's ability to accurately detect and assess them. Through all of this, the core mission of the IC will remain unchanged: to understand what is happening in the world, to deliver timely, accurate, and insightful analysis of those threats and developments to U.S. policymakers, and to provide U.S. leaders decisionmaking advantage over competitors. What will change is the IC's ability to fulfill this mission if it does not adapt to the new AI era.

The CSIS Technology and Intelligence Task Force set out to understand the emerging technology landscape, identify the opportunities and challenges to applying technology to intelligence missions, and generate recommendations that will enable the IC to adapt, integrate technology, and maintain an advantage over sophisticated rivals. The task force's research included dozens of interviews and deep-dive discussions with technology and intelligence experts across the IC, Department of Defense (DOD), Congress, private sector, and academia. Three key findings stand out:

1. **There is no shortage of opportunities to apply technology across intelligence missions *today*.** Technology is not just about the future. It can unleash significant improvements to intelligence missions right now. Opportunities include automating the tasking of technical collection platforms, enabling case officers to penetrate denied areas, augmenting analysts' ability to make sense of exponentially growing data, and delivering data-rich, visually engaging products to customers.

2. **The primary obstacle to intelligence innovation is not technology, it is culture.** The IC must overcome a host of institutional, bureaucratic, and policy challenges to adopting and integrating essential technologies the task force has identified. But at their core, many of these problems stem from an IC **culture** that is resistant to change, reliant on traditional tradecraft and means of collection, and—ironically, given popular perception—averse to risk-taking, particularly to acquiring and adopting new technologies and integrating outside information sources. In sum, IC culture must adapt to take and reward calculated risks.

3. **Failure to adapt will result in loss to adversaries and irrelevance to U.S. policy.** China and Russia, in particular, are moving rapidly to integrate emerging technologies into military and intelligence operations. In the race for technological intelligence superiority, the upper hand will go to those who innovate and adapt fastest. U.S. rivals enjoy a distinct advantage: unity of civilian-military effort and the consistent support of their technology sectors. The IC must also

adopt and assimilate these technologies to compete with alternative sources of intelligence for policymakers. The improving quality of open-source intelligence (OSINT), commercialization of space, and greater facility and ease in integrating AI and data analytics will enable private sector organizations to produce multisource intelligence that could rival or even beat the IC in terms of accuracy and relevance for policymakers—faster and cheaper. Failure to integrate these technologies will thus reduce the IC's ability to add value to what its "customers" have available from non-IC sources.

The IC today remains the global gold standard in intelligence. Until now, it has been able to execute its core missions of collecting, analyzing, and delivering intelligence without widescale use of emerging technologies, but this cannot continue if the community wants to maintain its superiority. With adversaries and competitors around the globe now adopting AI and other advanced technologies, the IC enters 2021 flatly behind the technology curve. Incremental reform to IC processes, marginal integration of AI, and occasional or ad hoc exploitation of big data will be insufficient to meet the mission; in fact, a piecemeal and episodic approach to technology adoption is a recipe for failure and eventual obsolescence.

Task force members believe there is a recognition of the IC's innovation problem among almost all of its agencies, key leaders, and outside stakeholders, along with an understanding that the stakes are high and the need for progress is urgent. In this final report, the task force aims to serve this common mission of driving intelligence innovation in several ways:

- Identifying specific, near-term "**applications**" of emerging technologies to advance three core intelligence missions: collection, analysis, and distribution;
- Highlighting six key "**enablers**" in which reform is necessary to facilitate technology integration: workforce and organizational culture; acquisition and adoption; strategic partnerships; strategic R&D; infrastructure and security; and ethics and governance; and
- Providing Executive, agency, and sub-agency level **recommendations** for action by the IC and its stakeholders.

The central theme of the report and the overarching conclusion of the CSIS Technology and Intelligence Task Force is that integrating emerging technologies into the current IC mission template is necessary in the short term but wholly insufficient over the long term. Rather, the dawning era of intelligence innovation must compel the IC to **reimagine** its tradecraft and missions to harness technology's potential and **reinvent** its processes, partnerships, workforce, incentives, and—yes—culture to embrace technological transformation.

Top Recommendations

A dramatic **reimagining** and **reinvention** of the IC will not happen without strong and consistent leadership from the top. Therefore, from among

more than 100 recommendations in this study, the task force recommends the new director of national intelligence (DNI) and IC leadership commit early to taking several major steps:

- **Launch an Intelligence Innovation Initiative:** This initiative should encompass many of the recommendations made in this report across the applications—collection, analysis, and distribution—and the associated enablers (Recommendation #44). The DNI should designate the principal deputy DNI (PDDNI) as the IC's senior official responsible for innovation and driving this initiative (R45).

- **Create an Intelligence Innovation Board:** Use this board to build strategic partnerships with technology, research, and venture community leaders and convene focused discussions on the latest trends in technology and their potential applications to IC missions (R58).

- **Refocus National Intelligence Priorities:** In collaboration with policymakers, use the National Intelligence Priorities Framework to raise the priority for science and technology (S&T) intelligence (R5). IC agencies should double the billets provided to S&T targeting and collection by 2023 (R4), elevate foreign S&T analysis to a core analytic discipline (R12), and establish a technology net assessment function focused specifically on emerging and disruptive technologies of U.S. adversaries (R81).

- **Establish a DNI Technology Investment Fund:** Work with Congress to ensure IC leadership has a significant, strategic, flexible, and multiyear resource pool to advance priorities and develop new, IC-specific capabilities, particularly in leap-ahead technologies such as biotechnology and quantum computing (R80).

- **Implement Post-Covid-19 Adaptation in the IC:** The Covid-19 pandemic has proven the IC can be agile and creative and break down barriers when necessary to continue executing the mission. It must not wait for the next crisis to spur such innovation. The IC should focus now on adapting organizational culture and enterprise architectures to remove obstacles to operating in cloud, mobile, and unclassified modes (R87).

- **Elevate OSINT as a core "INT":** This should begin with a study on how the IC's OSINT mission should be organized, to include the potential of a new OSINT agency (R25) and encourage IC agencies to integrate OSINT into collection and analytic tradecraft. For example, the CIA should establish an AI-OSINT Red Cell to test and demonstrate the utility of OSINT and AI in analysis on critical threats, such as the adversary use of AI-enabled capabilities in disinformation and influence operations (R10).

- **Reshape IC Human Capital:** This requires a new IC talent acquisition and management strategy that anticipates the core attributes of a premier IC workforce for the future and how the IC can attract and retain that force (R28).

- **Leverage the Closest U.S. Allies:** Announce efforts to build a Five-Eyes (FVEY) Cloud as the basis for technological collaboration, joint innovation, and intelligence generation and sharing (R72). Accelerate opportunities to collaborate with other allies and partners who are rapidly advancing AI adoption and integration, such as Israel, Singapore, and the Nordic countries, on intelligence innovation and mission applications.

SCENESETTER

Maintaining—if not increasing—a strategic intelligence advantage over increasingly sophisticated rivals and adversaries will be critical to ensure and advance U.S. national security interests. Central to this success will be the adoption and assimilation of emerging technologies such as artificial intelligence (AI) into the way intelligence is created and conveyed to decisionmakers. If intelligence is to provide U.S. leaders an advantage in formulating policy, then AI and associated technologies hold the potential to unlock deeper, wider insight and deliver it faster and more persuasively.

What Is AI?

For the purposes of this report, two definitions of artificial intelligence (AI) are particularly relevant—one from the national security field and the other from the commercial sector. AI is:

- **The ability of a computer system to solve problems and perform tasks that would otherwise require human intelligence, for example, recognizing patterns, learning from experience, drawing conclusions, and making predictions.**[2]
- **Systems that extend human capability by sensing, comprehending, acting, and learning.**[3]

These same technologies, however, will also transform the intelligence capabilities of strategic competitors such as China and Russia and those of weaker states and non-state actors and disrupt the very fundamentals of U.S. intelligence.[4] The U.S. application of these technologies will be a critical dimension of competition with such rivals. Indeed, how well and how rapidly the U.S. Intelligence Community (IC) integrates emerging technologies into the intelligence process and adapts to shifting threat and operating environments will be vital to its ability to generate and sustain policymakers' decisionmaking advantage.

While the challenges of emerging technologies to U.S. intelligence are formidable, the opportunities to harness them are greater. Over the past year, the task force has sought to identify opportunities to apply technology for intelligence mission gain, as well as the policy, legislative, organizational, technological, tradecraft, and cultural changes that must occur to effectively seize them. The task force's core objective has been to generate actionable recommendations to help the U.S. IC remain the global gold standard in producing strategic intelligence that provides policymakers advantages over U.S. adversaries. The core questions that have driven the task force's research year and this final report are:

- What are the opportunities to integrate advanced technologies into the generation of strategic intelligence? What are the foreseeable obstacles and how can they be overcome?
- What actions must the IC and its key stakeholders—policymakers, the U.S. Congress, the technology and industrial sectors, and the research community—take to ensure future advantage?

While envisioning and building toward future operating environments, the IC can and must harness emerging technologies to empower today's mission. Building off ongoing IC efforts, namely the Office of the Director of National Intelligence's (ODNI) Augmenting Intelligence Using Machines (AIM) initiative, this report intends to help bridge that continuum between current applications and future missions. Doing so will require IC leaders and stakeholders to provide the IC workforce with both the strategic direction and the necessary top cover to drive innovation and change. With that foundation, the IC can introduce the technology and training necessary to thrive in AI-enabled missions today while setting the institutional priorities, laying the digital groundwork, and establishing cultural norms for future success. Failure risks a reactive U.S. national security policy apparatus that is consistently unable to advance the nation's strategic interests in the face of chaotic information flows and determined adversaries.

This report is divided into three main sections:

- First, a **scenesetter** providing an overview of the current state of IC emerging technology adoption and the **strategic challenges** facing the IC;
- Second, an assessment of the near-term **applications** of technology to intelligence missions—collection, analysis, and distribution;
- Third, an exploration of the **enablers** that must be put in place now, such as rapid acquisition, digital upskilling of the workforce, and an intelligence innovation base, to continuously seize the opportunities technology provides over the long term.
- The report concludes with a review of the cross-cutting themes that emerged throughout the task force year.

STATE OF PLAY OF IC TECHNOLOGY ADOPTION

Emerging technologies are already reshaping how the IC gathers, processes, and evaluates information but will likely transform all core aspects of the intelligence process in the coming decades. Driving this change is the convergence of four technological trends, undergirded by the IC's previous investments in digital infrastructure:

- Massive growth in computing and processing power to process data and power AI systems, particularly through **cloud computing** and graphics processing units (GPUs)[5];
- Improvements in **AI and machine learning (ML) algorithms** and applications particularly suited to intelligence, such as computer vision and natural language processing (NLP)[6];
- Advances in networked **multimodal sensors**—systems able to collect data in different forms simultaneously—and the volume and quality of sensor-derived intelligence data; and
- Exponential growth in **big data** in the open-source domain—enabled through cell phone and internet penetration and social media—and advances in sophisticated **data analytics**.

This convergence of technologies—high-performance computing, cloud, advanced sensors, AI, and data analytics—holds tremendous potential to transform a host of critical intelligence missions and processes in the near term and is the focus of this task force (this set of technologies will be referred to as "AI and associated technologies" throughout the report). Other technological advances, particularly in space-based collection, additive manufacturing, quantum systems, 5G networks, robotics, miniaturization and nanotechnologies, and synthetic biology, will also transform the IC. These technologies will be touched upon in this report but merit further comprehensive study by IC leadership and other experts. (See Appendix A: Task Force Scope and Methodology for further details.)

THE URGENCY OF NOW

The U.S. IC today stands at the precipice of a new era of intelligence innovation powered by AI and its associated technologies. While the IC has thus far been able to execute its core missions of collecting, analyzing, and delivering intelligence without widescale AI adoption, those foundations are now shifting beneath the IC's feet as AI technologies are beginning to be adopted by actors and adversaries across the globe. The explosion of data and disruptive technologies, accelerating policymaker decision cycles, and rapid emergence of new global threats will likely upend traditional intelligence processes, tradecraft, and priorities.

- **Harnessing Data:** In a world of proliferating sensors and big data, the IC has an unprecedented capability to gather information of national interest. However, the sheer volumes of relevant data—classified and open-source—far exceeds analysts' ability to process it and turn it into meaningful insights. As sensor-derived and open-source data continue to grow, accelerated by the fielding of 5G and the Internet of Things (IoT) devices, the IC must be able to sift through, process, and synthesize this data into meaningful insight for further action.
- **Speed of Decisionmaking:** Leveraging AI and associated technologies to capture and analyze real-time and open-source data will be critical to the IC's ability to stay ahead of an accelerating information curve and provide timely analysis to decisionmakers. With the inevitable lags in clandestine collection, initial insights will often come from open-source intelligence (OSINT). Mastery of AI and data analytics will be vital to capture, connect, and make sense of vast streams of OSINT data. Failing to do so risks missing relevant information, providing an incomplete or erroneous threat picture, and being unable to deliver an accurate picture on the timeline policymakers demand.
- **Mission Enabling and Evolution:** Beyond "sensemaking" of big data, emerging technologies hold the potential to empower aspects of almost all current intelligence missions, enable the evolution of IC tradecraft, and help envision the next generation of intelligence missions for future operating environments. Enabling and evolving intelligence missions through technology will be vital—even existential—as the United States competes in the intelligence realm with adversaries seeking to deny the United States an information advantage.

When considering the opportunities presented by emerging technologies such as AI, it is also important to understand that these technologies are neither silver bullets to intelligence tasks and problems, nor independent from a much broader technology and human capital ecosystem.

STRATEGIC THREATS AND CHALLENGES

While the benefits of emerging technologies will be immense for American intelligence, their development will not occur in a geopolitical vacuum. U.S. rivals, China especially, but also Russia, are moving swiftly to integrate similar AI and associated technologies into intelligence operations. The challenge to U.S. intelligence, however, will come not only from U.S. adversaries. Foreseeable challenges will include the expanding number of threats the IC is responsible for assessing, IC bureaucracies and cultures that resist change, and the IC's diminishing primacy as the source of intelligence analysis for policymakers as the intelligence playing field is leveled between government and non-government organizations.

ADVERSARIES

The same technological tools augmenting U.S. intelligence will empower and embolden foreign intelligence rivals—principally China and Russia—in detecting, denying, disrupting, and deceiving U.S. intelligence. As the international race for dominance in AI accelerates, the battlefield will extend beyond the military realm and into the intelligence arena as AI and associated technologies permeate intelligence operations. In the evolution to "intelligentized" warfare, as Chinese military strategists describe it, China will enjoy a structural advantage: unity of civilian-military effort in developing and employing AI technologies.[7] This organizational advantage will be exploited to strengthen their defenses against U.S. intelligence operations and enable more targeted and aggressive offensive operations.

- **Unity of Innovation-Intelligence Effort:** China is betting that its whole-of-nation strategy for AI development, fusion of military and civilian spheres, and "techno-utilitarian political culture," as Kai-Fu Lee writes, "will pave the way for faster deployment of game-changing technologies."[8] This will provide Beijing a distinct advantage in fielding these technologies for intelligence missions at speed and scale. China, Russia, and other authoritarian states' abilities to synthesize civilian and military AI R&D and steer commercial sector innovation to military and intelligence applications enable them to pool national resources and know-how and potentially adapt technology more quickly to changing operational environments.[9] China's continuing advances in 5G and IoT will enable even faster collection, distribution, and use of AI-enabled intelligence tools, for both defense and offense.[10]

- **Stronger Defense:** AI-enabled intelligence tools will enable China, Russia, and other U.S. rivals to deny U.S. intelligence operations. A world of "ubiquitous surveillance" due to advances in smarter sensors, biometrics, and surveillance will create more denied areas for human intelligence (HUMINT) operations, a persistent risk of exposure, and the need to change or discard decades of well-honed tradecraft.[11] AI-enabled advances in cybersecurity and cryptography and, in the future, quantum computing could enable adversaries to harden and encrypt their systems to deny remote penetration of their networks.[12]

- **Aggressive Offense:** AI tools will also be exploited to penetrate, manipulate, and degrade U.S. intelligence, influence American political processes, or covertly shape U.S. society in detrimental ways. AI-accelerated cyberattacks will target collection and communication platforms and employ intelligent malware to access, exploit, or destroy critical data and intelligence.[13] Once inside, foreign intelligence could exploit adversarial AI to insert "poisoned" or false data into training sets to degrade IC algorithms and cause AI systems to fail.[14]

TARGETS

The IC needs clear intelligence priorities from policymakers to focus its planning, investments, and allocation of collection and analytic resources. But the increasing number and diversity of and rapid shifts in intelligence targets and security threats will make prioritization difficult. Indeed, the IC is balancing ongoing intelligence efforts involving great power rivals, malign regional actors, terrorism, and cyber threats with work on new targets such as bio-threats and global health during the Covid-19 pandemic. While emerging technologies can assist in these efforts, the technologies themselves will also accelerate many of the threats.

- **Disinformation:** As foreign disinformation and influence campaigns accelerate at unprecedented speed, scale, and seeming authenticity, the IC will be called upon to determine what is real, what is fake, and what impact it will have on U.S. interests.[15] U.S. adversaries will use AI capabilities such as generative adversarial networks (GANs) and natural language processing generate "deepfakes" of synthetic information and flood U.S. intelligence.16 It will be nearly impossible for IC analysts—and humans more generally—to detect the next generation of

inauthentic content without similar AI capabilities and deeper facility with open-source material.[17]

- **Science and Technology:** Foreign science and technology (S&T) capabilities, plans, and intentions have been less of a priority for U.S. collection and analysis than other traditional foreign intelligence topics, such as leadership, military, political, and economic intelligence. The IC must be able to understand and forecast emerging and disruptive technologies—particularly in AI, biotechnology, quantum computing, and space—and their applications to foreign statecraft, economic competitiveness, and military and intelligence operations.

- **Human Security:** The IC's capabilities in human security intelligence, such as global health and climate change, have been historically limited and occasionally sacrificed for other missions. As the Covid-19 pandemic has made clear, biology and biotechnology, among other human security challenges, will play a central role in U.S. national security in the coming decades.

"AI tools will also be exploited to penetrate, manipulate, and degrade U.S. intelligence, influence American political processes, or covertly shape U.S. society in detrimental ways."

CULTURE

IC agencies harbor deeply embedded institutional and cultural legacies, preferences, and biases that favor time-tested tradecraft and practices they perceive to be the global gold standard. These cultures have been vital to forging identity, shared sacrifice, and mission success but can also slow the pace of change and technological adoption.

- **Mission Siloing:** U.S. intelligence collection and analysis organizations have been designed around specific collection ("INTs") and analytic missions, building unique expertise and cultures over the decades. However, the blending of intelligence missions through the nature of AI and technological advances (e.g., HUMINT operators using their own signals intelligence [SIGINT] tools or AI-enabled SIGINT processing tools also generating analysis) could render such task organization irrelevant or ill-suited to future missions.

- **Preference for the Exquisite:** Harnessing AI capabilities will require embracing OSINT as vital analytic input and building trust in machine-derived results. Hindering this embrace is an IC bias for classified reporting in forming judgments, skepticism of OSINT—only growing with deepfakes and disinformation—as diagnostic data, and trust in time-tested tradecraft over algorithm-generated analysis. Preference for classified reporting may be appropriate, as a SIGINT intercept or HUMINT source may be the only way to discern plans and intentions. That preference, however, could leave IC analysts missing vital insights from open sources.

- **Aversion to Risk and Change:** AI investments require multiyear commitments from leaders to see through adoption and integration, acceptance of risk, and occasional failure. IC leaders, however, are often only in their positions for two to three years and may be unwilling to spend already strained time and resources on new technologies with uncertain mission payoff and a chance of failure, particularly if IC executives and oversight bodies do not incentivize such risk-taking. At the working level, operators and analysts with trust and confidence in traditional tradecraft are more likely to discard ill-suited technologies with unclear mission value than conform to them.

VALUE

The IC as currently constructed and operated is becoming less relevant, resulting in an erosion of its value proposition to U.S. leaders. The collection, analysis, and delivery of intelligence to U.S. policymakers is no longer the sole domain of the IC, as commercial and open-source data enable non-IC organizations to craft intelligence products in a way that is as timely, relevant, and accurate as what the classified intelligence world generates. Exquisite collection capabilities and the expertise of seasoned analysts will continue to distinguish IC products from

non-government competitors, but that advantage will erode if those products cannot meet policymakers' demands, interests, and timelines.

- **Commercialization of "All-Source":** The combination of high-quality open-source material, publicly available information (PAI), and commercial geospatial intelligence (GEOINT) and SIGINT will level the intelligence playing field between the public and private sectors. Combined with cloud-based AI, advanced analytics, and product distribution tools, any staffed and resourced organization will be able to generate multisource, if not **all-source**, intelligence analysis of comparable quality to IC analysts—at a faster pace and a fraction of the cost.

- **Vanishing Shelf Life of Secrets:** While exquisite collection platforms will still be needed to collect on hard targets and gather secret intelligence on plans and intentions, the persistent risk of hacks, cyberattacks, and leaks means these expensive tools can be more easily stolen, denied, and rendered inoperable by U.S. adversaries, negating their value. As one task force participant noted, the IC will likely face a "vanishingly short shelf-life of secrets," as its ability to keep its officers, operations, and information secret—as well as its monopoly on being able to access that information—will likely diminish in the coming years.

- **Perpetually behind Decision Cycle:** IC tradecraft, processes and standards, and a preference for assessments based on clandestine reports will ensure the enduring quality of IC products but also their potential irrelevance to U.S. policymakers if they arrive too late to impact decisions. 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 fast-moving global events, such as spontaneous mass protests, outbreaks of disease, or even military movements and operations. If the IC discounts timely, credible OSINT while it waits for clandestine sources to report, its analysts may fall behind and outside of policymakers' information and decision cycles.

APPLICATIONS

This section focuses on the task force's original primary objective, assessing the potential applications of advanced technologies such as AI/ML, cloud computing, advanced sensors, and big data analytics to intelligence missions. Rather than just assessing how emerging technologies can improve current intelligence tradecraft, the task force also explores how technology can and should **reimagine** and **reinvent** these missions in ways better suited to the technological-intelligence operating environments of the future.

This section summarizes the key findings of each of three formal phases of the task force study: collection, analysis, and distribution. It highlights the opportunities in technology for each mission, the obstacles or limitations to integrating technology, and the task force's recommendations for how to seize the opportunities identified and overcome the challenges.

This portion of the report concludes with a special section on OSINT—a topic that permeates the report but warrants a dedicated look, focusing on how the open-source enterprise can play a broader and central role across the intelligence mission enterprise.

COLLECTION

The IC exists to provide U.S. leaders advantage in a competitive global system. That advantage comes in many forms, including early warning, unique insight, reduced uncertainty, and increased confidence. Intelligence serves many customers, but its capacity is finite. Policy interests are documented as requirements and prioritized for intelligence producers. Once tasked, the intelligence professional turns their attention to cataloging what is already known and identifying sources that will inform a comprehensive response to the policymaker's request.

In a world of proliferating sensors and big data, the IC enjoys an unprecedented capability to collect intelligence of national interest—in more places, through more means, and at greater speed and scale than at any time in its history. Phase One of the task force revealed numerous opportunities for IC organizations to leverage existing, emerging, and imagined technologies to bolster collection missions.[18] However, Phase One also revealed the shortcomings of the **intelligence cycle**, which the IC has instinctively used to conceptualize and organize its missions, including collection, in the face of rapid technological change.

In the traditional intelligence cycle, intelligence is generated through a process of **tasking, collection, processing, exploitation/analysis, and dissemination** (TCPED). As policymaker requirements are documented and prioritized, the IC reflexively turns on its collection engine. Human sources are asked, communications are intercepted, and satellite images are tasked. Given the historic success of that model, this reliance is to be expected. However, this process is ill-suited to future and even current intelligence operating environments in several ways.

- First, in a world of ubiquitous sensing, answers to questions requested by policymakers may already exist in IC holdings. During the Cold War and early part of the twenty-first century, the amount of information on the IC's shelves was small relative to the number of questions decisionmakers were posing. As the world has become more continually sensed, the information at hand or readily accessible has become voluminous and is growing every day. The tasking of scarce, expensive, or risky IC collection assets can be avoided in many instances.

- Second, the information required to answer their questions may not require dedicated IC collection and assets at all. The growing availability, quality, and relevance of unprotected data and OSINT—from commercial imagery and signals collection to social media and financial data—means that intelligence once only acquired through clandestine and high-end technical collection can be derived from unclassified and publicly available information.

- Third, TCPED infers, and sometimes dictates, a linear process. While the actual process is iterative and less sequential, it risks a bigger problem—linear thinking. The world's growing interconnectivity demands that such thinking is dynamically challenged.

Given the exponential growth in available and accessible data, the IC must adapt the traditional intelligence cycle to today's information environment. After an IC organization is **tasked** to respond to a baseline question but before its **collection** assets are engaged, the organization must identify and **survey, scan, and search** through existing data that satisfy a policymaker's requirement, both inside the IC and in the outside world. This means reviewing current intelligence holdings and sifting through OSINT and unprotected data streams to find answers, or partial answers, to a given intelligence question before proprietary

technical or human assets are tasked. To realize the full potential of this vast unprotected reservoir of information, the IC should acquire the tools, tradecraft, and culture to surface, vet, and value open-source information and the new insights it can unlock. This acquisition should be in partnership with industry and academia.

As part of this cultural shift, the IC must also overcome the false comfort that comes from reliance on proprietary collection resources. Too often, the IC defaults to this collection to the exclusion of open-source alternatives because the IC already has it, understands its provenance and associated confidence levels, and knows how to use it. The risk of this default position is the missed opportunity for novel insight. Moreover, the more systematic exploitation of unprotected sources would also reduce costs, risks, and demands on clandestine collection assets.

The **collection** phase in a new, adapted intelligence cycle would be grounded in the routine exploitation of open-source data using emerging technologies. The IC's exquisite, proprietary means of collection would henceforth be focused on filling the most persistent intelligence gaps, such as the hostile intentions and plans of America's state and non-state adversaries.

Opportunities for Collection

Technical Collection: When U.S. collection assets are needed, the IC must leverage emerging technologies such as AI, multimodal sensors, cloud computing, and advanced analytics to automate how platforms are selected and tasked, sharpen and specify what is collected, and tailor processing tasks to user needs.

- **Adaptive Tasking:** AI tools can assist in automating the planning, scheduling, and tasking of collection platforms and optimizing asset selection.[19] Advances in deep learning could enable more rapid, adaptive tasking of collection assets with limited need for human involvement.[20]

- **Signal Detection and Early Warning:** Technical collection can harness advances in ML and sensors to detect more types of enemy signals, identify imperceptible changes in target environments, and sense anomalous or high-risk behavior. Such AI-enabled signal detection and search models could be integrated into indicators and warning systems automated to "tip and cue" collection.[21]

- **Automated Processing:** AI can help automate, expedite, and streamline the processing of exponentially growing technical collection data. For GEOINT, computer vision already assists in processing streams of imagery and video data and performs more complex human tasks, such as image recognition and categorization.[22] NLP can transform a variety of SIGINT processing and previously human tasks, including speech-to-text transcription, voice identification, text summarization, and language translation of intercepted communications.

- **Triage and Notification:** AI can also "triage" and sort the IC's massive data and information flows for information collectors and analysis, freeing analysts to spend more time on tasks requiring higher-level thinking.[23] ML algorithms could be honed to comb large data sets, such as from imagery and SIGINT collection, for information prioritized for specific analysts. AI tools could also be trained to spot and flag information designated as critical and send automated alerts to the analysts and decisionmakers.[24]

- **Pattern Recognition and Sensemaking:** Analysts must employ deep learning algorithms to identify patterns and trends in data streams, make inferences on relationships between targets, and visualize networks for enhanced clarity and deeper meaning.[25] As AI tools progress, the back-end result of better data processing could be better and automated data sensemaking delivered in digestible and actionable forms for both collectors and analysts.[26]

HUMINT Collection: Early task force discussions also revealed the pervasive impact of emerging technologies, in particular digital advances, on the HUMINT discipline. While operations officers are still able in many cases to apply traditional tradecraft in the recruitment and handling of human sources, digital technology is rapidly transforming the most tradition-laden intelligence discipline.

- **Agent Acquisition:** In training HUMINT professionals and managing field collection operations, specialists often refer to an **agent acquisition cycle** that includes: spotting potential sources with access to the desired information, assessing a target's suitability as a source, developing a personal relationship, recruiting the target to commit espionage, and handling the agent through secure means of communication. High technology has for decades supported secure communications with agents, but the more recent global spread of the

"While operations officers are still able in many cases to apply traditional tradecraft in the recruitment and handling of human sources, digital technology is rapidly transforming the most tradition-laden intelligence discipline."

internet, proliferation of portable devices, and allure of social media has impacted every phase in this cycle. Indeed, as terror groups and state adversaries have demonstrated, it is possible to spot, assess, recruit, and direct agents without any personal contact.

- **Offense and Defense:** The race to apply emerging technologies to HUMINT operations has both offensive and defensive implications. Mastery of emerging technologies will allow HUMINT officers to securely collect unique information from sources with natural access to the plans and intentions of America's state and non-state enemies. Simultaneously, U.S. adversaries are exploiting the same commercial, adapted, or bespoke technologies to, for example, defeat U.S. officers' cover identities, surveil their movements, and intercept covert communications with reporting sources.

- **Counterintelligence:** Moreover, authoritarian societies have an advantage on the defensive side by virtue of the tighter control they maintain over internet access and social media; this enables them to protect officers' identities and mask cover arrangements more readily than open, transparent societies such as the United States. Equal attention should be paid to the role technology can play in helping U.S. intelligence agencies mount espionage operations and defend U.S. officers and information from hostile foreign services.

Challenges for Collection

The IC's ability to harness these technologies in support of the HUMINT mission faces numerous internal obstacles and challenges detailed later in the report, including the speed of tech acquisition, skill sets of collection professionals, and organizational cultures around them. But perhaps the greatest obstacle to tech-enabled U.S. intelligence collection will be the capabilities and countermeasures of adversaries. The same technological tools augmenting U.S. intelligence will empower and embolden foreign intelligence rivals, prominently China and Russia but also others, to detect, deny, and degrade U.S. HUMINT.

- **Detection:** Accelerating use of smart sensors, surveillance, and biometrics will transform intelligence operating environments into ones of "ubiquitous surveillance"—not just in authoritarian states such as China and Russia but even in neutral or allied countries across the globe. As high-counterintelligence (CI) threat areas proliferate, officers will struggle to maintain cover and operate clandestinely and face a persistent risk of exposure—of themselves, their agents, and their operational tradecraft.

- **Denial:** AI-enabled advances in cybersecurity and cryptography will help adversaries to harden and encrypt their systems and complicate U.S. efforts to penetrate and collect on their networks.[27] For HUMINT collectors, intensifying and sophisticated hostile surveillance from CI services could provide the host nation persistent, pervasive coverage of U.S. officers, complicating denied area agent communications.

- **Degrading:** Hostile foreign intelligence services could exploit AI to put technical platforms under persistent threat by penetrating, manipulating, and degrading collection. AI-accelerated cyberattacks could target collection and communication platforms and employ intelligent malware to access, exploit, or destroy critical data and intelligence.[28]

Recommendations: Adapting to Evolving Threat and Collection Environments

Emerging technologies hold tremendous potential to augment, accelerate, and improve the way intelligence is collected and processed to better serve U.S. national security objectives. In the iterative competition for technological-

intelligence advantage, no single set of technologies will ensure the United States gains and retains the advantage over sophisticated adversaries and rivals. Rather, what will be decisive to mission success is the **adaptability** of collection missions, tradecraft, and operations to contested operating environments and the **speed** at which they field and integrate innovative technology to enable and transform those missions.

- Acting as the IC's HUMINT mission manager, **the director of the CIA, in consultation with other IC leaders, should direct multiple pilot initiatives designed to test the current and likely future impacts of emerging technologies on HUMINT operations (Recommendation 1, hereafter R1)**. The pilots should address doctrine, human capital, training, cover, field platforms, technology requirements, investments, and experimentation, as well as the role of OSINT in tradecraft and operations, among other areas.

Defeating the Hardest Targets: The IC must invest in technologies that enable collection and operations into denied areas and clandestine and covert missions in a world of ubiquitous technical surveillance. With so much knowledge of global activity available in OSINT and non-clandestine means, the IC must focus collection on penetrating hard targets and collecting vital information on adversary plans, intentions, and capabilities that otherwise cannot be detected.

- At the strategic level, the directors of the CIA and the undersecretary of defense for intelligence and security (USDI&S) should co-lead an IC **advanced tech-enabled hard target strategic planning initiative (R2)**. This should assess the likelihood and impact of ubiquitous surveillance and advanced countermeasures on intelligence operations and the capabilities needed to defeat them. The initiative should include partners at the leading edge of relevant technology in industry, start-ups, and academia for more purposeful, hard-target-centric investments. The goal will be to establish an R&D investment base for exquisite capabilities that is connected to operations in both the near and long terms.

- At the operational level, the IC should empower, staff, and resource director of national intelligence (DNI) Representatives in the foreign field to assemble forward collection teams to push AI-enabled collection and analysis closer to operators in contested areas (R3). Comprised of case officers, technology small and medium-sized enterprises, data scientists, and SIGINT and GEOINT analysts with reachback capabilities, these forward fusion teams would enable more rapid and adaptable collection plans and operations.

Elevating Technical Intelligence (TECHINT): Intelligence of foreign AI systems and S&T capabilities, plans, and intentions must be conceived as a core collection mission alongside other foreign intelligence. Doing so will require clandestine collection of adversary technological capabilities and applications, along with well-sourced OSINT of foreign S&T sector innovation

- IC collection agencies—particularly the CIA and NSA—in coordination with Congress, should aim to **double the billets provided to S&T targeting and collection** of emerging and disruptive technologies by 2023 (R4).

- The Office of the Director of National Intelligence (ODNI) should facilitate a focused discussion with the White House to **raise the priority assigned to S&T in the National Intelligence Priorities Framework (NIPF)**—the IC's key intelligence planning documents—and in agency-internal collection requirements (R5).

Next Generation CI: As noted in the September 2020 report of the House Permanent Select Committee on Intelligence (HPSCI) on the IC's capabilities toward China, "[i]n tandem with Beijing's increasing military and technological clout, China's intelligence services continue to threaten the safety and security of U.S. personnel and national security information."[29] Already sophisticated, persistent, and pervasive, China's high-tech espionage campaign against the U.S. national security and commercial sectors, among many others, will be augmented and accelerated with AI and other emerging tech. In fulfilling its national security mandate, the IC must bolster its CI capabilities—both technical and personnel—to stay ahead of the CI threat.

- The ODNI, through the National Counterintelligence and Security Center, should review the current capabilities of the IC's China-focused CI cadre and what skill sets will be needed, including Chinese language capabilities and understanding of emerging tech, to counter the next generation of CI threats (R6).

Understanding the Potential of Biotechnology: Although not a primary focus of the task force, synthetic biology, its convergence with AI and computational power, and possible intelligence mission applications such as biosurveillance

and remote sensing with biological systems stood out as having a potentially transformational and generational impact for the collection of intelligence. It is also an area fraught with concerns over ethics and global norms.

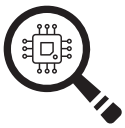
- The ODNI, in partnership with the National Academy of Sciences, should **sponsor a study on the potential intelligence collection applications and implications of synthetic biology** and associated technologies (R7).

Processing Upstream: Even with enhanced processing capabilities in collection organizations, the exponential growth in the IC's sensor-derived data may still overwhelm its ability to process. Sensors embedded with AI models would be able to pre-process the data or only send back information flagged as important for customers, reducing information flows and the strain on bandwidth, particularly in harsh edge environments.

- IC collection agencies should **invest in AI-embedded sensors** to pre-process and sort collected data "at the edge" or at the point of collection, reducing the latency and amount of information transmitted to users. This can allow collection agencies to shift processing from rote sorting tasks to more advanced applications with computer vision and NLP and move more tasks to automated sensemaking (R8).

Scope Note on Technology and Covert Action

The task force recognizes and acknowledges here that many of the same emerging technologies that are so profoundly shaping the core intelligence functions (information collection, analysis, and distribution) also impact covert action activities. Covert action is defined in statute as government activities "to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[30] An executive order assigns the conduct of covert actions to the CIA, where supporting activities are undertaken by operational, technical, and support officers using existing and custom platforms. Successful covert actions, such as intelligence operations generally, often depend on the development, adaptation, and application of technology. Many of the lessons and recommendations in this report will apply equally to covert action. For example, the same tools that may enable intelligence exploitation of large social media feeds emanating abroad may also be useful in tailoring covert influence messages aimed at the platform's users. For scope and classification reasons, the task force study did not address covert action and emerging technologies notwithstanding the topic's similar importance and urgency.



ANALYSIS

The explosion of data and disruptive technologies, rapid evolution of global threats, and accelerating policymaker decision cycles will upend the intelligence analysis process. How well and how rapidly the IC integrates emerging technologies into all-source analysis will be vital to its ability to generate timely, relevant, and accurate strategic insights and sustain policymakers' advantage over capable rivals. Phase Two of the task force examined how AI and associated technologies can augment analysts' ability to deliver high-level and value-added intelligence to customers as well as the host of barriers and limitations—in the underlying data, algorithms, and, ultimately, the analysts themselves—that must be acknowledged or overcome.[31] Moreover, while AI can enhance what information is presented to customers and how analysts present it, it neither can nor should automate or replace the role of analysts and their vital judgment and contextual knowledge.

Opportunities

AI cannot replicate all the complexities of crafting strategic analysis but can automate, enhance, and enable key parts of the analytic process. 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, assist analysts to make sense of exponentially growing data, unlock new insights to inform judgments, and create more **strategic bandwidth** for analysts to think and write strategically.

- **Optimizing Intelligence Traffic:** AI tools can help surface the most relevant and useful information in analysts' ever-growing "traffic" queues—from sensor data and signals intercepts to diplomatic cables and social media. Recommendation algorithms could be used to find and flag reporting of interest based on the analyst's strategic portfolio and immediate policymaker needs.[32] Advances in ML, particularly NLP, could enable algorithms to cluster and summarize vast streams of reporting on key topics that analysts could otherwise never fully read, providing a jump start on identifying emerging trends and generating products.[33]

- **Augmented Detection and Sensemaking:** With intelligence sifted and streamlined, AI and analytics can help analysts make sense of it to identify and visualize patterns and changes in their target environments.[34] AI can help analysts detect incremental changes in the daily intel churn, which, unnoticed, can culminate in strategic surprise and intelligence failures.

- **Offloading Analysis:** AI can also **perform** certain types of analysis, enabling analysts to offload or outsource work done as ably or better by machines. Analysts can use AI and NLP tools to generate machine-derived analyses from large bodies of unstructured text, such as news articles and diplomatic cables, and create first drafts of certain products.[35] This includes machine-generated geopolitical and foreign conflict updates, social media data mining for stability and crisis monitoring, and AI modeling for political and economic forecasts.

- **Testing Analytic Lines:** Analysts could harness technology to refine and test their analysis against machine-derived insights. While unable to simulate analysts' cognition, contextual knowledge, and critical thinking, AI can surface contrary data, measure historic accuracy, and posit alternative hypotheses. IC leaders could require analysts to address countervailing machine analysis before advancing their products for review and publication.[36]

The combination of emerging technologies, human subject matter expertise, and IC tradecraft would leave IC analysts uniquely positioned to answer the difficult, often technologically oriented questions that policymakers will pose in the coming years:

- **What is new?** As U.S. competitors increasingly adopt irregular, indirect, and clandestine approaches short of war to gain strategic advantage, AI and multi-INT fusion and visualization tools could enable analysts to better understand and anticipate such gray zone activity. Analysts with AI-enabled signal detection, pattern finding, and visualization tools combined with traditional expertise on adversary strategy and doctrine will be more likely 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 is true?** As AI-enabled disinformation and influence campaigns intensify and accelerate, policymakers will turn to the IC to help separate truth from fiction. Analysts will need AI capabilities to detect synthetic and inauthentic deepfakes and use sentiment analysis to measure influence operations' impacts. Analysts with both technical skills and country expertise will be ideally suited to assess adversaries' information warfare strategies and potential future operations.

- **What is next?** Anticipatory strategic intelligence is about correctly assessing the likelihood of potential events and adversary actions. AI-enabled modeling, wargaming, and scenarios analysis could help analysts to 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. Just as critically, the teaming of analysts and algorithms will enable the better leveraging of human judgments in domains where AI models currently underperform, such as causal reasoning.

Limitations

While the benefits of AI and associated technologies could be immense for analysts, the IC faces limitations in applying these tools. The broad challenges of technology acquisition, digital infrastructure, and data architecture identified in the "Enablers" section of this report will be part of the problem. But structural barriers are not the primary obstacle. AI's own limitations in matching analysts' standards of tradecraft and explainability with the cultural and institutional preferences of analysts and agencies for traditional approaches will be the primary obstacles.

- **Keeping Pace with Data:** Even with AI-enabled visualization and streamlining, the proliferation of sensors and OSINT data—accelerated by 5G and IoT devices—could still overwhelm analysts' capacity to process. If this happens, IC analysts will be behind the curve in providing situational awareness to policymakers.

- **Algorithmic Limits:** The complex tradecraft of strategic analysis depends on rigorous processes and clear explanations and reasoning of the logic, evidence, assumptions, and inferences used to reach conclusions. The intricacies of strategic analysis, involving the role of informed human judgments, and requirements for transparency and assurance pose real challenges for modeling analytic processes and practical limits to

applying AI to analysis. Moreover, the "brittleness" of AI—it functions poorly, and in strange ways, when slight boundary conditions change—and the bias and opacity inherent in certain algorithms and models will also constrain AI's applicability and usability in the analytic processes.

- **Analytic Aversion to Change:** Deeply embedded preferences for time-tested sources and methods, underinvestment in digital acumen, uncertainty of AI and OSINT's mission value, and cultural aversion to change could hinder even the most innovative analysts and units from integrating emerging technologies into their mission.

Recommendations: Enhancing and Demonstrating Mission Value

The IC's ability to integrate technology into strategic analysis will be vital in delivering decisionmaking advantage to U.S. policymakers over adversaries and rivals. Doing so will require effective teaming of analysts and algorithms and integration of the strengths of each into how analysis is generated. AI's immediate value to analysts and analysis is in answering the what—that is, to capture, connect, and make sense of vast streams of data on what is happening with an analyst's country, issue, or target of interest. Where technology lags is in answering the why. Understanding the drivers, intentions, and motives of foreign actors and the history, context, and personalities shaping their actions remains the unique strength of human experts. An analyst armed with the AI and OSINT to make rapid sense of what is happening, and the secret intelligence and historic context to know why, will be able to provide unmatched insight on global threats, future scenarios, and implications for U.S. policy. What will this require?

Automating the Mundane: As the IC navigates the complexities of tech integration, the IC should look for the low-hanging fruit of immediate AI applications as a means to demonstrate value and spark change. One key area is in automating vital but tedious and time-intensive knowledge management tasks, such as curating, collating, and cataloguing exponentially growing intelligence traffic.

- IC analytic agencies should move rapidly to procure, adapt, and integrate commercial off-the-shelf AI applications using ML and NLP for traffic optimization, summarization, and categorization (R9). This should proceed while being cognizant of and working to mitigate potential security risks and performance shortfalls with commercial AI.

Demonstrating Mission Success: IC leaders should empower and coordinate with individual directorates and mission centers to acquire, experiment with, and adopt the tools that fit their mission needs. Certain analytic missions, particularly more operational intelligence-focused ones such as counterterrorism (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. A clear demonstration that successfully applies AI and OSINT to real-world analytic problems in areas such as nuclear proliferation, terrorism, or CI will recruit converts faster than any paper or speech.

- The CIA Directorate of Analysis should establish an **AI-OSINT Red Cell**, equipped with cutting-edge AI tools, access to data and data scientists, and training to test and demonstrate the utility and application of AI/ML technologies and speed up technology risk mitigations where needed (R10). The cell could focus on a vexing problem set that is conducive to OSINT and AI analytics, such as **foreign disinformation campaigns**. If successful, the cell may be the IC's "early adopter" that builds momentum for AI to scale across analytic mission centers.

Embracing OSINT: While experimenting with an OSINT Red Cell, IC mission centers must simultaneously move to integrate OSINT into analytic processes and tradecraft. Analysts should view OSINT as a foundational "INT" alongside traditional clandestine intelligence collection in informing and driving analytic judgements. OSINT is the area where application of AI and ML can show early success, largely because OSINT is so vast and so in need of careful curating. A key objective would be to enhance timeliness and relevance to policymakers and to understand what they may already have absorbed from independent access to open-source data so as not to duplicate that in reporting. Analysts should focus on integrating what they learn from open sources with other aspects of big data and with secret intelligence to produce the most complete picture of adversary plans and intentions.

- **IC analytic directorates and mission centers should move swiftly to increase analysts' abilities to access OSINT and PAI reporting on unclassified systems**

"AI's immediate value to analysts and analysis is in answering the what—that is, to capture, connect, and make sense of vast streams of data on what is happening with an analyst's country, issue, or target of interest."

that are integrated into their classified workspaces (R11). The ideal AI applications for analysts would be able to integrate both classified and OSINT data in AI models and algorithms, a challenge addressed in the "Infrastructure, Architecture, and Security and Assurance" section of this report.

Integrating TECHINT: Analysts have long assessed the S&T behind foreign weapons systems and defense industries. Going forward, it will be equally important to assess adversaries' S&T innovation in AI and other emerging tech domains and integrate those findings into strategic political and military analysis of those actors. As IC analysts become more knowledgeable and adept at employing AI and other technologies, their expertise could enable deeper insights and analysis of adversaries' S&T plans, intentions, capabilities, and threats.

- IC agencies with regionally focused analytic mission centers should establish **foreign S&T as a core analytic discipline**, alongside military, political, leadership, and other key areas, and integrate S&T analysts into country analytic units (R12). Particularly with regard to China and Russia, line analysts should be empowered to directly liaise with IC open-source experts on foreign S&T, including at In-Q-Tel, Intelligence Advanced Research Projects Activity (IARPA), and ODNI bodies and initiatives recommended elsewhere in this report.

Leverage the Wisdom of Crowds: The IC can benefit by expanding its use of prediction markets and similar crowdsourcing tools. Currently, the IC Prediction Market (ICPM) is the only tool that allows the IC to systematically collect forecasts from across the community, spot points of disagreement, and assess accuracy on a broad range of intelligence questions. In head-to-head comparisons, the ICPM has been more accurate than traditional analytic methods; it aggregates knowledge that is broadly distributed and cancels out errors by combining large numbers of diverse judgments.

- Assuming the continued successful operation of the ICPM, the National Intelligence Council (NIC) should create a new product line for the NSC that includes quarterly updates on key strategic questions posted to the ICPM (R13). Most key judgments in NIC products should also include a forecast from the ICPM.

- IC analytic components should sponsor "forecasting tournaments" that compare human judgments, AI models, and combinations of the two to forecast real-world events (R14). One team competing should be all-OSINT, for comparison against forecasts derived primarily from classified intelligence. The accuracy of intelligence analysis should become an empirical matter rather than just a speculative one.

Educating Policymakers: Analytic value ultimately derives from a product's impact on policy customers and their trust in its quality, clarity, and transparency in explaining its judgments. As the IC moves to integrate AI and data analytics into its products, this may be largely invisible to customers. Analysts must be able to clearly and convincingly explain to policymakers the role of AI and analytics in generating their analysis and their impact on confidence levels when these technologies have been instrumental in the process. Analysts will need to become educators on AI and analytics applications as part of building trust with strategic leaders making policy and operational decisions based on their AI-enabled analysis.

- The CIA's Sherman Kent School for Intelligence Analysis should add to its curriculum for analysts a module on educating policymakers on the use of AI in intelligence analysis as part of preparation for interacting with senior policymakers (R15).

DISTRIBUTION

Emerging technologies can help transform not only the crafting of intelligence but also how it is delivered to decisionmakers—at the time, place, and level needed to have impact and stay ahead of the decision curve. Beyond product dissemination,

cloud and AI tools can help transform how intelligence is shared and delivered more broadly between analysts, organizations, and allies to distribute vital knowledge and inform decisionmaking.

Opportunities

Creating: AI and other emerging technologies can assist analysts and briefers in how they assemble daily products for customers, answer new taskings, and test and strengthen the analysis they present in briefings and products. While AI can automate and augment **how** intelligence is presented to customers, the role of the analyst and their vital judgment and the context of customer needs must remain central in deciding what intelligence is presented.

- **Tailored Knowledge Bases:** Analysts can harness AI and Wikipedia-like knowledge bases to capture, tailor, and update standing assessments and operating pictures of importance to their customers, with clear exposition of the reporting and content driving those judgments. ML models could recommend reporting to include as analysts build their brief and be automated over time to self-update with new intelligence.[37] Briefers armed with customized knowledge bases on mobile secure devices will be able to instantly provide customers standing assessments by topic and dive deep into specific questions on the spot.

- **Answering Taskings:** When customers issue taskings, analysts can expedite the process of answering them with AI applications using NLP to find existing data and products relevant to the question and condensing them into a draft product tailored to the policymaker's requirement.[38] Harnessing NLP summarization can not only save time for analysts but strengthen their analysis by drawing on multiple and diverse products and insights.[39]

- **Surfacing Gaps and Contrary Views:** Instead of gearing algorithms to analyst preferences, AI systems could be instrumented for the opposite—finding reporting that disconfirms human analysis or is outside their customary source base, helping mitigate confirmation bias and the risk of missing valuable reporting. AI could help generate non-intuitive analytic alternatives and run contrary hypotheses and estimates to inform, test, and ultimately strengthen what analysts are presenting to policymakers.[40]

Delivering: As cloud and AI are distributed and used across IC and policymaking organizations, analysts should be able to better time, tailor, and target products to diverse sets of consumers according to their unique intelligence needs.[41] Global cloud capabilities could also help analysts deliver customized intelligence to more decisionmakers—military, diplomatic, and intelligence operators as well as non-government customers—in more places around the world, unlocking new customers for their products.[42]

- **Maximal Impact:** AI can enhance analysts' awareness of what intelligence customers value, measuring trends in product consumption, why certain pieces are trending, and predicting what products users would be interested in based on their attributes.[43] Smart distribution tools can help analysts both broaden their customer base and tailor their products toward users where the intelligence could have the most impact.

- **Rapid Targeted Dissemination:** For more operational decisionmakers, AI and cloud computing could enable automated and targeted delivery of critical, time-sensitive intelligence to users with "need to know" based on their attributes (e.g., rank, role, and location).[44] Delivery could become more precise over time, using advertising technology tools and techniques for the microtargeting of alerts and breaking events or steady-state customized content to customers, even down to the individual level.[45]

- **Expanded Customer Base:** Cloud computing and AI could also be leveraged to deliver intelligence to customers outside the traditional Washington customer base. Multilayer fabrics and cloud architectures could enable the IC to more easily and securely share intel with diplomats, military, and law enforcement at different classification levels across the globe.[46] Outside government, cloud and data sanitization tools could assist the IC in sharing sensitive but unclassified information with the private sector on matters of vital importance, such as cyber threats to critical infrastructure and disinformation campaigns on social media platforms.[47]

Consuming: Much like AI can help analysts process and prioritize relevant reports, these tools could help consumers prioritize which intelligence products they receive and customize their daily readbooks to serve their current policy and operational needs. Personalized intelligence products, visual storytelling technologies, and mobile

secure platforms could enhance the **intelligence user experience** and enable customers to consume intelligence in ways uniquely optimized to them.

- **Tailored Products:** For the IC's more senior customers, such as recipients of the President's Daily Brief (PDB), analysts and algorithms can team-build customer profiles that leverage ML to assemble tailored readbooks that curate and customize content based on the customer's portfolio and event calendar, travel schedule, and other unique needs.[48] Between briefing sessions, AI could produce a personalized recommendation list of additional products or new reporting and suggest articles based on what other customers with similar attributes are reading, as well as products with alternative and divergent judgements and sourcing.[49]

- **Engagement and Feedback:** AI-enabled products and briefings can be further honed via engagement and feedback tools and user data analytics. AI models and digital interfaces can be instrumented to measure how customers engaged with a product and content within it and enable customers to provide direct, measurable feedback on quality, timeliness, and relevance of content.[50] Customer engagement and feedback can be further enhanced by embedding conversation features in products or, for senior customers, allowing them to connect with the author in real-time to answer questions.[51]

- **Visualization and Immersion:** Analysts and briefers can leverage interactive graphics, animation, and, in the coming years, augmented reality and other immersive technologies to transform how policymakers consume analysis.[52] Transitioning solely from dense written products to more visual storytelling will enable the IC to present intelligence in a way more conducive to how customers actually intuit and digest complex information.[53]

- **Mobile and Secure:** The combination of AI and mobile secure edge devices could help analysts "meet the customer where they are" and allow policymakers to securely access intelligence content wherever and whenever they need it. Notification algorithms based on user preferences or contextual variables such as current time, location, or upcoming meetings could be enabled to securely deliver alerts and content. AI could also assist with redacting, formatting, and delivering the content at lower classification levels as needed.

Challenges and Risks

- **Customer Confirmation Bias:** It is the IC's duty to tell policymakers what they **need** to know, not just what they want to know. Too much customization and use of recommendation algorithms risks policymakers' optimizing their intelligence queue for analysis and reports that support or confirm their preferred assessment of the situation, in support of their policy objectives. Analysts must remain in the loop to curate content and ensure they are delivering—albeit smarter and more tailored—"truth to power."

- **Trust of User:** The use of AI for customized intelligence will first require analysts to cultivate relationships with their customers to gain the level of access, context, trust, and buy-in needed for technologies that instrument and monitor their engagement and feedback. The human element, however, is too often missing, as many analysts do not know their policy customers, which could leave policymakers reluctant to allow their consumption habits to be modeled and analyzed.

- **Machine-Readable Feedback:** To leverage AI for customized intelligence delivery, the IC will need to be able to digitize and instrument all aspects of the analyst-customer dialogue and have sufficient customer data to model and perform predictive analysis—both of which the IC currently lacks.[54] As one IC official noted, the "n" for the number of IC customers and their associated data "is not 1 but is still very small," which could hamper the ability to use AI to train tailored intelligence systems.[55]

- **Disconnected Networks:** For both specialized customer delivery and broad, rapid dissemination, the lack of integrated networks, data, and architecture across intelligence creators and users will slow or prevent the use of many AI applications.[56] The IC's default network policy of "security by isolation" will hinder connection of intelligence to users and the digitization of analyst-customer interaction and feedback.[57]

Recommendations: Intelligent Customer Service

Emerging technology such as AI, cloud, and associated mobile hardware can help reimagine and reinvent how the IC serves the intelligence needs of its customers. But technology itself is no panacea; indeed, for tech's greatest potential uses—timed, tailored, and targeted products and

customized user experiences—it will be the traditional, personal, human relationships between analysts and customers that enable those applications. Transparency and trust will be essential.

Closing the Feedback Loop: Truly harnessing AI for intelligence distribution will require re-instrumenting the process of product delivery, consumption, and feedback to build models that accurately reflect the level of customer engagement and direct, real-time feedback on product value for policy and decisionmaking. Getting customer buy-in from the outset will be vital.

- Many of the recommendations of the recently released Center for American Progress report on embracing business data analytics are sound regarding improving the efficiency and effectiveness of feedback for IC products.[58]
- The ODNI, in conjunction with intelligence production staffs such as the PDB, should initiate a study on what changes to data architecture, engagement metrics, and customer modeling will be required to apply AI and data analytics to customer feedback while maintaining customer confidentiality (R16). The findings should be briefed to senior policymakers at the National Security Council (NSC), Departments of Defense and State, other PDB recipients, and Congress.

Voice of the Customer: The IC must find a way to facilitate the trust and confidence of customers in technology experimentation and ensure policymakers' priorities are better integrated into how both analysts and algorithms decide what content to generate. Educating the IC's most important senior customers on the benefits of AI could help demystify concerns and demonstrate the value to decisionmaking.

- The IC should develop an emerging technology training course, or **AI boot camp, for senior leaders** and intelligence customers (R17). Developed and hosted at a Federally Funded Research and Development Center (FFRDC), university, or think tank, the course would center on how AI could be used in intelligence analysis, briefings, and customized products and on the implications of AI-informed intelligence for policy and decisionmaking. The course should also clearly lay out what levels of instrumentation of policymaker engagement and consumption habits will be required as well as the attendant risks and benefits.
- Policymakers should also take a more active role in telling the IC which products and delivery tools are most useful. The White House should more routinely issue Presidential Decision Directives (PDDs) that establish intelligence production priorities, identify what technologies should be enhanced, promulgated, scrapped, or developed, and send a clear demand signal for incorporating AI and OSINT into finished intelligence products (R18).

IC SkunkWorks: The IC must be equipped—and incentivized—to test and experiment with cutting-edge technologies that could enhance the intelligence user experience. And beyond just products, analysts should be empowered to be creative in harnessing technology to deliver their services to policymakers and the rest of the community, particularly during fast-breaking events. Strategic analysts often dislike acting as a "classified CNN," but technology could enable more effective and engaging ways to do so and ensure their timeliness, and thus relevance, to policy.

- The IC should **establish an intelligence experience "skunkworks,"** bringing IC production staffs, briefers, and analysts together with data science, data visualization, virtual reality/augmented reality (VR/AR), user interface/user experience (UI/UX), and mobile device engineers and experts to create, test, and evaluate innovative products and services (R19).
- IC production teams, such as the PDB or CIA WIRe, should **develop an "Analyst Live" broadcast channel** for senior analysts and authors of new products to provide real-time video analysis of current events (R20). The broadcasts could be classified or unclassified, enabled for desktop or secure mobile devices, and have comments and threads for community-wide discussion, including with policymakers. "Live" analysts could have on-hand access to other tools and technologies referenced in this report, such as real-time automated OSINT summary and analysis, to stay updated and react during broadcasts.

Engaging Non-PDB Customers: The goal for analysts is not just to reach the right policymakers but for their analysis to have impact on policy and decisionmaking. However, too much of the IC production enterprise—and how analytic performance is measured—is focused on the PDB and NSC principals and deputy-level customers. Not enough attention is paid to the mid-level policymakers—from desk officers and country directors to assistant secretaries and

ambassadors—and other senior consumers who inform, shape, and execute national security policy on a day-to-day basis, such as U.S. combatant commanders.[59] At the same time, working-level policymakers may lack daily access and awareness of IC products as well as general familiarity with the IC and the go-to analysts and teams for their issue set.[60]

- IC agency leaders should incentivize mission centers to encourage and reward analysts for **cultivating relationships with mid-level policy customers** and working with production staffs to exploit emerging technologies for digital delivery and engagement (R21). IC organizations routinely serving policymakers at the secret and unclassified level, such as the State Department's Bureau of Intelligence and Research, should be the leading edge of experimentation and implementation.

- IC analytic agencies should leverage emerging technologies to deepen partnerships with key non-PDB customers, focusing on common and serious intelligence needs, such as a common operating picture in key theaters, intelligence sharing with host-nation and coalition partners, and sorting out what is "real" and "not real" for influence operations (R22).

Smart and Secure Distribution

The IC's ability to distribute timely and impactful intelligence to the right customer at the right time is beholden to a classification and security system accepting of zero risk and deviation from protocol. Decisions on "need to know" and dissemination are often dictated by security personnel with little experience or contextual knowledge for speed and urgency of intel-driven decisionmaking and operations. While the security challenges and justifications are important and real, the IC must find ways to harness AI and advanced security technologies to distribute intelligence to users who need it. The IC's "duty to warn" is a vital mission and one that must expand outside traditional customer sets to military operators on the ground, U.S. commercial entities battling cyber threats, or foreign allies and partners.

- The ODNI should assess the benefits and risks of using AI/ML for instantaneous decisions about distribution—determining "need to know" based on user attributes (e.g., location, echelon, time horizon) instead of traditional classification accesses and labeling—and develop a pilot program to test a new distribution model (R23).

- The ODNI, with assistance from In-Q-Tel and IARPA, should explore investments in **distributive ledger and blockchain** technology for enabling rapid intelligence sharing outside IC networks in zero or near-zero trust environments, such as the U.S. private sector and foreign liaison (R24).

SPECIAL SECTION ON OSINT

The task force has concluded that the IC must fundamentally reconceptualize OSINT as a cornerstone of U.S. intelligence, relevant across the IC enterprise and in all aspects of its current and future missions. Unlike the other "INTs," however, OSINT does not have a dedicated agency. The IC's Open Source Center (OSC) currently resides in the Directorate of Digital Innovation at the CIA. Not a single task force commissioner believes an OSC subordinated to one directorate at one agency is the right place to harness OSINT's potential impact across the government. Before assessing where the optimal placement is, it is useful to first review what missions and functions the IC should have OSINT and the OSC (or a successor) fulfill:

Input to Classified Intelligence: The growing quality, relevance, and timeliness of OSINT is now fundamental to all-source analysis. OSINT should be conceived as a foundational INT for strategic intelligence, on par with information collected from classified means (e.g., HUMINT, SIGINT, GEOINT). OSINT can also play a critical role in tipping/steering/driving classified collection when needed.

Unclassified Finished Intelligence: The combination of cloud, cloud-based AI and analytics tools, and commercial

"Educating the IC's most important senior customers on the benefits of AI could help demystify concerns and demonstrate the value to decisionmaking."

GEOINT and SIGINT collection means that high-quality, multisource intelligence analysis can be produced at the unclassified level from anywhere equipped to do so. As the Covid-19 pandemic has clearly demonstrated, OSINT and enabling technologies can allow the IC workforce to keep functioning in remote unclassified environments and delivering high-value insights even when outside a Sensitive Compartmented Information Facility (SCIF). Cleared analysts could serve a vital bridging and communications role between the OSC and IC agencies. They could target and tee up the work of open-source analysts for relevant IC analytic teams while vetting and validating major OSINT findings with classified ones to ensure they are not wildly divergent and off-base

Customer Service: The IC should also embrace OSINT as a means to expand its reach and impact with a variety of consumers with unclassified intelligence products. From U.S. diplomats and defense attachés, to domestic law enforcement, to tech and social media firms battling cyber and disinformation threats, to American voters, a wide range of customers and stakeholders would value actionable insights informed by superior IC tradecraft but delivered at the unclassified level.

Foreign Liaison: An expanded OSINT mission is particularly well suited to building intelligence partnerships with foreign liaisons. Instead of just sharing intelligence, U.S. OSINT analysts could collaborate with foreign counterparts in building assessments from the ground up. Alongside analysts, data scientists and AI experts could partner to test, train, and develop algorithms and applications. In addition to the Five-Eyes (FVEY) intelligence alliance, OSINT liaison partnerships with innovative services with common security threats such as Israel, South Korea, Japan, and the Nordic/Baltic states are ripe for expansion.

Public Voice: The IC's ultimate customer is the American people. An empowered OSINT agency could serve as the IC's public voice, demonstrating its value to citizens increasingly disillusioned with U.S. institutions and perceiving the IC as a "deep state" hostile or alien to average Americans and their interests. Instead of a singular annual Worldwide Threat Assessment, an OSINT agency could more routinely engage and share vital intelligence with American citizens on global trends and threats likely to impact them.

Innovation Lab: An OSINT agency could serve as a proving ground for emerging technologies and a test lab for algorithms and applications of potential use in classified intelligence missions. It would serve as the IC's natural bridge for substantive engagement with the commercial tech sector, enabling IC analysts to learn about emerging technologies and tech developers to see potential applications, or "slipstreams," of their technologies to IC analytic missions. In addition to the private sector, an empowered open-source entity could also be a vital link to American universities, non-government research institutes, think tanks, and other research organizations.

Talent Acquisition: An empowered OSINT agency could expand its geographic footprint across the United States and even in select allied countries. Similar to DIUx, creating OSINT hubs near top tech talent centers (e.g., Pittsburgh, Austin, Atlanta, and the San Francisco Bay Area) could produce high-quality OSINT while serving as natural incubators of tech talent. They could also serve as a de facto holding area and early training ground for would-be IC professionals whom the IC might otherwise lose to disastrously lengthy clearance processes.

Recommendations

Accomplishing the OSINT functions and mission sets above will require an open-source organization able to: provide inputs and insights to analysts and operators across the IC; produce all-source unclassified analysis; deliver such analysis to an array of government, commercial, academic and foreign customers; and possibly expand its geographic footprint to domestic tech hubs. At its outset, the task force did not envision—and indeed sought to avoid—a "box-moving" exercise and calls for IC reorganization, focusing instead on how the current system could better harness technology. It has become clear, however, that the transformative potential of OSINT, as a vital element of IC workflows and tradecraft and an interface with the open-source world, cannot be reached in the OSC's current auspices. The task force considered a number of options for the OSC, including:

Option 1: Establish an Independent Open Source Intelligence Agency (OSIA)

Congress and the IC establish the OSIA as the 18th U.S. intelligence agency, independent from the CIA.

- **Pros:** Keeps OSINT tethered to daily IC processes and clandestine assessments while still able to perform many, if not all, of the missions and functions described above.
- **Cons:** Creating a new agency almost from scratch. Even championed by an independent agency, OSINT

may never be able to thrive inside IC culture that preferences classified data.

Option 2: Move the OSC to the State Department

This option keeps the OSC inside the IC but assigned to an executive department with clear mission value and overlap, such as the Department of State. The OSC would serve the State Department's public diplomacy mission while still playing an active part in IC production, technology development, and the nurturing of outside partnerships.

- **Pros:** Easier, direct, unclassified interface with commercial and research sectors. Under policymakers who more generally rely on unclassified information and are most likely to use OSINT products. Supports broader challenges for the U.S. government in using OSINT to support public diplomacy that have existed since the demise of the U.S. Information Agency. Still able to provide IC analysts OSINT reporting and products.
- **Cons:** OSINT unlikely to become foundational to IC missions if outside and unintegrated into daily IC processes and products. The IC will not accrue the benefits of the OSINT and AI revolution if the government's center for excellence is outside of the community.

Option 3: Move the OSC to the ODNI

Move and establish the OSC as a standalone center under the ODNI, similar to other centers (e.g., the National Counterterrorism Center).

- **Pros:** Able to serve all IC agencies and policymakers without the internal pressures of being under a single agency. Synergies with the ODNI, as it is already the IC hub for innovation, outreach, and public engagement.
- **Cons:** The ODNI is meant to serve a coordinating role, not house a major collection, analysis, and distribution center.

The task force was unable to reach a consensus on one of these options. The task force instead recommends that the ODNI, in conjunction with Congress, commission a specific study on the IC's OSINT mission (R25).

- In the interim, the ODNI should designate an OSINT lead to spearhead an IC-wide, cross-functional effort focused on driving and improving the integration of OSINT into IC tradecraft, workflows, and analytic products (R26).
- Regardless of which option for the OSC is pursued, the task force recommends the IC establish unclassified OSC forward offices near key technology and talent hubs, starting with the San Francisco Bay Area (R27). OSC forward offices could be co-located with existing IC facilities, enabling a small number of IC managers with clearances and access to IC networks to keep OSC efforts tethered to IC work.

ENABLERS

Technology and innovation per se are not the obstacles to IC transformation. As the "Applications" section of this report described, there is no shortage of relevant emerging technologies and potential ways to apply them to enable and empower intelligence missions. Rather, the IC's long-term success will be determined by its ability to overcome a host of other challenges—institutional, bureaucratic, technical, policy, and cultural—that will impede technology adoption and intelligence transformation if left unaddressed.

To overcome these challenges, the task force identified six key areas—or "enablers"—that must be established, emphasized, reformed, or wholly reimagined for the IC to seize the potential of emerging technologies. These enablers include:

- An IC **workforce and organizational culture** trained and incentivized to apply new technologies;
- **Acquisition** processes that rapidly distribute cutting-edge technology to users for **adoption** and mission integration;
- **Strategic partnerships** with the commercial sector, research community, and foreign partners to ensure an American and allied innovation base supportive of IC needs;
- Investment in **strategic R&D** for gaining advantage in leap-ahead technologies;
- A robust IC **infrastructure and architecture** to exploit technology; and
- A clear framework of **ethics and governance** principles to guide how technology is applied to U.S. intelligence.

WORKFORCE AND ORGANIZATIONAL CULTURE

Within intelligence organizations are intelligence professionals; in an AI-augmented workplace, who will be recruited and attracted to join the IC? At the same time, how will non-tech-savvy career officers be retrained and retooled to succeed? Will case officers and political analysts who spent a decade studying Arabic, the Middle East, and specialized HUMINT tradecraft also need to learn how to code? The fundamentals of what an intelligence professional is and does is going to change dramatically. Current officers will be required to prepare for a tech-driven future while still mastering present day missions and tasks. New officers who are digital natives will have to adapt and assimilate into organizations and cultures that are moving unevenly on the path to harnessing their tech talent.

Seizing the tech-enabled opportunities outlined in the "Applications" section will require a workforce that is trained, organized, equipped, and incentivized to do so. Before making recommendations, it is worth first describing what technology-eager intelligence officers are up against. While dozens of different intelligence roles and disciplines are essential to the IC, three types of officers will be particularly critical to technology adoption for mission application: collectors, analysts, and technologists.

Collectors—Wedded to Tradition: The next generation of case officers will need to arrive with or acquire significant S&T skills to operate or lead effectively in digital collection and agent-handling environments.[61] However, in the HUMINT world, one task force expert noted that a "romanticism" continues to surround traditional field tradecraft. "Institutional resistance" to change still impacts how case officers are recruited, trained, and rewarded, hindering the speed and depth at which digital skills are inculcated into officers and operations. Current case officers who have excelled in the traditional aspects of the HUMINT tradecraft have struggled to adjust to an environment where digital technology is central to the process of spotting, assessing, recruiting, handling, and vetting human sources.[62]

Single-source-based collection and analytic organizations such as the National Geospatial-Intelligence Agency (NGA) and the National Security Agency (NSA) remain largely centered on the specific skills and tasks that have defined them for decades, relegating new disciplines such as data scientists and ML engineers to second-tier roles.[63] Effective analysts at technical collection agencies such as the NGA and NSA will need to continue mastering highly specialized skills such as signals, imagery, and geospatial analysis while gaining literacy and baseline skills in AI/ML and analytics tools to integrate into their analysis.[64]

Analysts—Aversion to Change: 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

"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 customer."

but supportive leaders and management that value and incentivize it. However, analysts and managers alike are often skeptical of new technologies and tools that promise transformation as well as of the suggestion that their analytic tradecraft and skills are somehow insufficient. Analytic managers will also need to balance investment in digital proficiency with traditional tradecraft, language, and other region-specific training that will still remain vital to the IC's analytic advantage.

Training, incentives, and leader support may still not be enough to spark technology adoption if analysts and managers see no clear and substantial "mission gain" from technology. Marginal gains in insights and productivity may not justify the time, expense, and opportunity cost required to gain AI proficiency. Analysts may also be offered too many technical tools to see the value of any, particularly when they are not designed and tailored to their unique analytic needs.

Technologists—Out of the Mission Loop: The IC's cadre of technical officers, including data scientists, ML engineers, technology researchers, and S&T targeters, among others, serve many critical and useful roles across the IC enterprise. But many of them and their vital skill sets are not integrated into the day-to-day execution of core intelligence missions such as foreign intelligence collection, all-source analysis, and covert action. Moreover, IC technologists often lack the same clear career tracks as their operations officer and analyst counterparts and do not have clear paths to reach senior agency leadership levels.

IC Wide—Insufficient Diversity, Equity, and Inclusion: Diversity, equity, and inclusion (DEI) is mission-critical for success across the IC enterprise and in ensuring the IC workforce reflects the people of the nation it serves. But DEI is particularly vital for the adoption of AI in identifying and reducing the biases that a homogenous workforce would otherwise introduce into data selection, algorithm development, and model design.[65] Despite its ongoing efforts, the demographic profile of the IC workforce, and its AI/ML specialist cadre, does not match that of the American people.

Recommendations: Retooling, Refreshing, and Retraining a Tech-Savvy Workforce

Emerging technology adoption may change the tools available to collectors and analysts but not necessarily their organizational cultures and leadership attitudes toward which skills and missions should be prioritized and valued. IC leaders and stakeholders—policymakers, Congress, and the technology and research sectors—must provide the IC workforce the technology and training to thrive today while laying the digital groundwork, institutional priorities, and cultural norms for future success.

Building off the work of the ODNI AIM Initiative, the IC should articulate **a new IC talent acquisition and management strategy** that determines the core attributes of a premier IC workforce for the future and how the community can attract and retain that force (R28). It should explore, among other topics:

- What levels of digital literacy and technical skill sets are needed for the AI-enabled intelligence tasks of the future;
- How the IC can better recruit, incentivize, and integrate STEM-focused professionals into core missions; and
- How the IC should retrain and retool the existing workforce to prepare for a tech-driven future.

Recruitment: Diversifying and enhancing the IC talent pool will require being able to tap into talent in every corner of the United States and outside the traditional "ivory tower" recruitment base. It should also build off other national security workforce efforts, particularly at the Department of Defense (DOD).

- The CIA Directorate of Operations (DO) and other HUMINT organizations should prioritize hiring candidates with existing STEM capabilities alongside

enduring priorities such as foreign language and cultural expertise (R29).

- All-source analysis organizations should emphasize recruiting candidates with STEM backgrounds, particularly those who also have education and skills in key regions and functional areas (R30).
- The IC should increase the number of IC positions requiring only secret clearance, particularly in technical fields, and unclassified positions focused on open-source information, to help acquire talent that is unable or does not want to receive a Top Secret/Secret Compartmented Information (TS/SCI) clearance. Potential OSC forward offices, as mentioned in the OSINT section, could be an excellent place for such talent (R31).
- The IC should continue virtual internships and externships, including during the academic year (R32). These are important hiring pipelines for those outside the Washington, D.C. area and without the financial means to move to and live in the area. Off-site interns and externs should be afforded equal opportunities to those working onsite in earning a full-time position after graduation.
- The IC should establish "STEM pay," similar to foreign language pay, and hiring bonuses for any IC employee using STEM skills in their day-to-day mission (R33).
- The IC should explore with Congress and the DOD the potential for graduates of the recently proposed U.S. Digital Service Academy and STEM Corps to join positions in the IC, including agencies outside DOD agencies, such as the ODNI and CIA (R34).[66]

Skills and Training: IC leaders must take stock of the current and anticipated future workforce and determine which roles—particularly in collection and analysis—will require what level of digital and AI skills and training, across the spectrum from digital **awareness** to **literacy** to **fluency**. The goal should be AI and digital awareness for all officers and tailored (and evolving) courses for officers seeking literacy and fluency based on career preferences and mission need.

- The IC should, even before training operators and analysts, also prioritize digital literacy for contracting and procurement officers, budget analysts, and security personnel, who are often the ultimate deciders of technology acquisition (R35). This training should include best practices in DevSecOps, modules on how AI and other tools are to be applied to missions and understanding of how these officers fit—and buy—into tech transformation.[67]
- The U.S. HUMINT community should urgently develop and field-test new doctrine and train the next generation of officers in the tradecraft required to securely collect intelligence from human sources in a fully digitized world (R36). DO field tradecraft courses should include training on AI and associated technologies and integration into operations, including simulations and exercises.
- The curriculum of the CIA's Sherman Kent School for Intelligence Analysis should be adapted to develop baseline digital literacy for all analysts and expanded training in data science, ML, and AI applications for analysts seeking to regularly apply these tools (R37).
- The IC's STEM cadre should receive more extensive education and training on core collection, analysis, and covert action missions and how STEM skills and capabilities can be integrated (R38).

Teams and Tradecraft: Analysts and case officers 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 intelligence missions. IC mission centers must integrate their talent and skills into the daily mission space.

- The CIA, Defense Intelligence Agency (DIA), and other all-source analysis organizations should establish an **Analytic Team of the Future** initiative, envisioning how to integrate technologists into analytic units to hone and tailor AI applications for analysis and evolve analytic tradecraft (R39).

Career Tracks and Retention: Building a premier IC digital workforce will have the unfortunate externality of making those officers more attractive to the private sector. The IC cannot compete on salary but can retain and advance a tech-savvy workforce by offering an irreplaceable mission and the opportunity for mission impact. At the same time, IC agencies must provide opportunities for technology experts to build careers, grow their skill sets, and find exciting opportunities to serve the mission outside of headquarters.

- The CIA should continue to build out the recently established CIA Labs for many reasons, including its

creative approach to allowing open-agency officers to take credit for their innovation and IP through patents and global recognition (R40). CIA Labs is both a great way to spark IC entrepreneurship and demonstrate to innovators their value to the enterprise.

- IC HUMINT organizations should establish an S&T case officer cadre, with specialized training and mission assignments focused on collecting intelligence on foreign S&T plans, intentions, and capabilities (R41). S&T case officers should have a similar path to senior DO leadership positions as any other cadre.
- All-source analytic organizations should similarly establish AI analyst cadres, focused on assessing foreign AI systems and S&T capabilities and their integration into statecraft, economic competitiveness, and military and intelligence operations (R42).
- IC organizations, particularly the CIA, should expand the opportunities available for S&T targeters, data scientists, and researchers to serve in overseas assignments as well as in locations across the United States. Such positions would serve as both a means to retain their talent with exciting assignments and to better integrate their skills into operations (R43).

ACQUISITION AND ADOPTION

Crossing the "valley of death"—taking promising technologies from early-stage development into widespread operations and adoption by the workforce—remains a perennial challenge. Exacerbating this challenge is the continued divide between users and technology providers as well as the growing divergence in both processes and timelines between the IC's acquisition and adoption cycle and that of commercial sector technology innovators. The community's lengthy procurement, testing, and evaluation timeline reflects its unique missions and applications, legitimate risks, and security requirements. But it also reflects the IC's continued reliance on some obsolete ways and means for acquiring and integrating technology, ill-suited for the pace of technological change.

In short, the U.S. IC cannot compete in the global intelligence arena and fulfill its vital missions without a reinvention of how it procures, adopts, and assimilates emerging technologies and delivers them to mission users—at speed and at scale. The task force has identified several key priorities and numerous recommendations for both IC leadership and mission levels to implement needed change.

Prioritize IC Innovation: The importance of IC executive leadership in establishing priorities, driving change, and communicating that change, both internally to the workforce and externally to key stakeholders, cannot be overstated. The workforce—be it senior managers, analysts, or acquisition officials—is less likely to seek out new technologies, experiment with their application, and incur potential risk without express support from leadership. This starts with a clear articulation by leadership of the necessity for change, the benefit that emerging technologies can bring to IC missions and problems, and the prioritization that leadership places on the acquisition and adoption of these technologies. Internally, this prioritization manifests itself through persistent leadership messaging and implementation across policies, programs, personnel, and budgets. Externally, IC leaders must prioritize easing the restrictions and general reluctance of IC personnel in engaging the private sector, largely due to the classified and sensitive nature of its work and enable and encourage the workforce to discuss its technology needs with the commercial and research sectors.

In short, IC executive-level leadership must make innovation a top institutional priority.

- The **DNI should establish and announce a new Intelligence Innovation Initiative (I3)**, articulating the urgency, mission benefits, and senior leader commitment to innovation and change across the IC through rapid acquisition and greater adoption of emerging technologies (R44).

Many of the recommendations outlined in this report could nest under this Intelligence Innovation Initiative, but a few executive-level elements are important to include:

- The DNI should definitely designate the principal deputy director of national intelligence (PDDNI) as the IC's senior official in charge of innovation across the IC, and the innovation portfolio—the scope to be determined by the DNI—as the PDDNI's top priority (R45).
- The DNI and PDDNI should review the roles and missions, staffing, and organization of the ODNI to ensure it is optimized to drive a coherent, strategy-driven approach to catalyzing innovation across the IC (R46).

- The ODNI should expand the IC's strategic partnerships with the U.S. technology and manufacturing sectors, to include establishing a new Intelligence Innovation Board (discussed further in the "Strategic Partnerships" section of this report).

- The PDDNI, working with agency leaders, should develop an innovation risk framework that aids organizations in weighing both the risk of failure/loss and the opportunity cost of inaction when considering acquisitions and adoptions of innovative new capabilities (R47).

Refresh the IC's Acquisition Tool Kit: There remains a fundamental mismatch between the IC's traditional, linear acquisition process and timelines and the realities of the dynamic and more iterative software development and operations cycles. This mismatch extends to the process and timelines of the planning, programming, budgeting, and execution cycle. While the IC retains flexible acquisition authorities, these authorities are not sufficiently used and implemented to match the speed and best practices of the software development life cycle and to meet rapid-changing mission and user needs. For example, one software firm the task force interviewed cited a 10-month-long timeframe from contract award to on-contract, while another cited 2.5 years from requirements to task order to initial delivery.

- The PDDNI should lead a comprehensive review to refresh acquisition and requirements policies and practices, to include software-specific policies and practices, rapid contracting, and flexible authorities, and to incentivize greater risk-taking and exercising all available current authorities where they already exist (R48).

- IC leadership should further develop a new software acquisition model to guide agency procurement and pilot a "software as a service" model inside a mission agency. The IC should adopt many of the best practices outlined in the Defense Innovation Board's Software Acquisition and Practices (SWAP) study (R49).[68]

- The IC should continue to develop flexible acquisition authorities, including through further examining an IC Acquisition Consortium approach with authority to provide IC-wide contract vehicle(s) for agencies to leverage (R50). These pathways can provide a focused expertise in software acquisition, rapid contracting, and performance measured in timeliness.

- The IC should prioritize training of contracting officials on rapid authorities and new approaches for procurement of software, AI, and associated advanced technologies (R51).

Integrate IC and DOD Acquisition Strategies: There are opportunities for the IC to both learn from the DOD's creative and entrepreneurial approaches for its acquisition and implementation strategy and to leverage the DOD's resources through joint partnerships and collaboration.

- The DNI and the secretary of defense should establish a Tri-chair Steering Committee on Emerging Technology across the DOD and IC, consisting of the PDDNI, deputy secretary of defense, and vice chairman of the joint chiefs of staff. This was also recommended by the National Security Commission on Artificial Intelligence (R52).[69]

- The ODNI and USDI&S should partner to catalyze DOD-IC collaboration forums for further integrating initiatives and sharing of best practices and lessons learned, to include an annual DOD-IC AI summit and annual DOD-IC acquisition conference (R53).

The task force examined DOD's AFWERX and SOFWERX public-private partnerships among models for building greater innovation ecosystems with the emerging technology sector, academic, and non-traditional partners. These models aim to bring entrepreneurial approaches and new technology solutions to bear against national security problems. They also emphasize prototyping, experimentation, and deeper collaboration between users and technology providers for rapid capabilities delivery

- The ODNI should examine options for creating an ICWERX, housed under ODNI CTO, as a premier innovation and procurement hub with sufficient resources and personnel. Alternatively, or in addition, the IC could establish cells in other hubs such as AFWERX and SOFWERX to combine investment resources with DOD elements where priorities align (R54).

Bridging the Innovator-User Divide: While the IC must rapidly procure commercial off-the-shelf software and AI technology, those technologies are more likely to be adopted if users, acquirers, and providers are aligned from the beginning of the process. Innovators must know the needs of the user, the user must know what technologies are available to augment the mission, and procurement officers must understand the true user requirements as

well as the software development process and timelines of the providers. All parties must be able to swiftly adjust course as mission needs shift and the operating environment changes. Educating users down to the mission center level can be useful in enhancing focus on emerging technologies and intelligence applications and enabling clearer and more targeted mission statements, requests, and feedback to acquisition officers and technology developers.

- IC leadership, under the auspices of the Intelligence Innovation Board and In-Q-Tel, should facilitate more regular and direct conversations between mission directorates and technology providers (R55). With acquisition officers in the loop, dialogue could focus on creative and collaborative discussions on current and expected future mission requirements, which technologies can meet them, how those technologies could transform and reinvent missions, and how to find the right UI/UX for intelligence officers.

- IC leadership should, in balancing risk tolerance, encourage agencies and directorates to pursue a rapid prototyping approach, more quickly pushing out prototypes and "beta" versions of software and other technologies for user feedback and continuous iteration, instead of waiting for the 100 percent solution before deployment (R56). Agency leadership should identify a major program or system as a "pathfinder" for AI adoption. This will require working with industry partners on data rights, contract modifications, and application programming interfaces (APIs) to open the system to vendor-agnostic AI solutions.

- IC agencies should encourage integrating technology providers and procurement officers into user experimentation, wargaming, modeling, and simulations to help develop intelligence-operational concepts with emerging technology experts (R57).

Build Digital Infrastructure at Scale for IC-wide Accessibility: Another primary limitation to widespread adoption of emerging technologies is the IC's digital infrastructure and the processes that allow for the rapid integration of data and applications onto IC networks. To its credit, the IC has been a leader across the federal government in its embrace of IC-wide IT networks (with IC IT Enterprise, or IC ITE) and cloud capabilities. It must continue to build on this foundation with further scaling of its digital infrastructure, including steps to make large-scale classified and unclassified data available in the cloud, including training data and data conditioned for ingestion by AI systems. It must also create secure environments for the development, test and evaluation, and operations of AI systems where classified intelligence data is utilized, as well as processes to enable the rapid accreditation of software for IC-wide usage. The task force's recommendations on this topic are discussed in the "Infrastructure, Architecture, and Security and Assurance" section.

STRATEGIC PARTNERSHIPS

Commercial Sector, Research Community, and Foreign Partners

The emerging "AI era" is unlike any previous era of U.S. defense and intelligence innovation, in ways that could prove daunting for the IC and its ability to harness emerging technologies for numerous reasons:

1. The United States no longer dominates the global market in creating the cutting-edge technologies such as AI that will be applied to defense and intelligence missions.

2. The IC can no longer assume, as it did during the Cold War and post-9/11 era, that the leading U.S. innovation firms will support the IC mission and provide them the best, game-changing American technology.

3. Much U.S. critical national security infrastructure resides outside the U.S. government, leaving the backbone of IC missions in the hands of the private sector.

4. Most if not all of the emerging technologies in this era are inherently dual-use, creating powerful private sector incentives to develop and sell them to foreign markets.

5. These technologies are "born open," not secret, making them widely available to individuals, organizations, and countries outside the United States. As a result, many of the usual government tools that have worked in the past, such as classification and export controls, are ill-suited to sustain national advantage in the AI-era.

The U.S. IC and its stakeholders must begin to strategically build a robust **intelligence innovation ecosystem** with like-minded partners outside the IC to provide the technology, people, and expertise to power a tech-enabled IC in the transformative days and decades ahead. Doing so will require the IC to, among other efforts, build **strategic**

partnerships with key stakeholders and innovators outside the IC—namely the commercial sector, research community, and foreign partners. It will also require coordinating those efforts and investments with the IC's own **strategic R&D**, with particular focus on the next-generation of game-changing technology, covered in the next section of the report. Indeed, the IC's strategic partnerships and technology investments must seek to balance between technologies with near-term applications to intelligence missions and those that will be necessary to gain future advantage.

Commercial Sector

The private sector will be the primary source of innovation for many, if not most, of the near-term technologies analyzed in this report. For AI and its associated technologies, these commercial firms include major U.S. technology giants, traditional defense and intelligence firms (producing both hardware and software), the U.S. investment and venture capital sector, and the hundreds of smaller start-ups and companies offering AI products and expertise. The IC must be able to find, engage, and establish relationships with all parts of this diverse commercial innovation ecosystem.

Beyond just procuring technology, the IC must build deep and sustainable partnerships with the private sector to ensure both sides can better serve each other and adapt to ever-changing waves of new technologies, operating environments, and IC needs. Unlike previous eras, the IC will need to be a "fast follower," rather than primary creator, of cutting-edge technologies now predominantly developed in the private sector. The IC must stay apprised of cutting-edge commercial technologies, communicate its needs to supportive firms, and convince their key stakeholders and investors that serving the IC is a profitable and otherwise worthwhile pursuit.

- The IC should establish a **U.S. Intelligence Innovation Board (IIB)**. Housed under the ODNI, the IIB would be a convening forum for tech sector, IC, research, and venture community leaders and experts to discuss the latest trends in emerging technology and potential applications to the IC mission set. The IIB would meet quarterly and be expanded to include standing committees and working groups that could meet more frequently on specific technology and mission areas (R58).

- The ODNI CTO (a new role recommended in the "Strategic R&D" section of this report) and In-Q-Tel should create a unified **IC venture engagement strategy** for interacting with the U.S. venture capital community to access, adapt, and deploy innovative technology, led by In-Q-Tel.

Deeper partnerships and regular engagement between the IC and commercial sector would enable more optimal fielding of new technologies and serve a variety of critical IC mission needs, from data and talent acquisition to information on global technology trends. Given its technical expertise and experience with the private sector and venture capital community, In-Q-Tel should serve as the primary interface for these engagements. At the same time, IC leaders must change outside engagement policies to allow for direct engagement between knowledgeable IC analysts, scientists, technical experts, and the private sector. While such engagement between IC professionals and commercial providers poses some risk, it is the only way to ensure innovators are truly connected to operators.

Rapid Customized Fielding: While the IC must procure and assimilate commercial off-the-shelf AI technology, those tools and applications will be more rapidly operationalized if they are designed from the beginning with UI/UX tailored to IC users.

- In-Q-Tel and the ODNI should host a biannual **UI/UX forum** that brings together software and application designers from firms supporting the IC with IC technology end users to test and solicit feedback on UI/UX for intel applications and products being developed (R60).

Assessments of Disruptive Technology: As the IC seeks to strengthen its foreign S&T intelligence capabilities, in part to inform its own investments, it must leverage the commercial sector and venture community's deep knowledge and expertise in global technology.

- The IIB, In-Q-Tel, and OSC should convene an annual **Worldwide Technology Threat Assessment** conference for the IC and private sector firms focused on assessing emerging and disruptive technologies (R61). The IC, under the NIC or OSC auspices, could additionally craft an unclassified assessment of the key findings. Congress could hold a Technology Threat Assessment hearing to align legislators and garner greater attention to these issues.

Data and Algorithm Sharing: In addition to software and platforms, the IC also needs data from the private sector and better ability to acquire and access large volumes of commercial data sets to test, train, and power AI/ML algorithms and applications.

"The IC must be able to find, engage, and establish relationships with all parts of this diverse commercial innovation ecosystem."

- Through the IIB, the IC should explore the potential for more robust data and algorithm development and sharing with select, vetted private sector partners, particularly in the financial sector, commercial imagery and other space-based collection firms, and data analytics firms (R62).

Talent Sharing: Bridging the divide between technology producers and IC end users could be accelerated through talent exchanges, rotations, and experiential learning opportunities for IC professionals and private sector innovators. While outside the IC's typical risk tolerance for outside engagements, the reward would be an IC cadre better connected to cutting-edge technology development and best practices and private sector partners with a deeper understanding and appreciation for IC mission needs.

- The ODNI should establish an Intelligence Innovation Fellowship that selects 8 to 10 IC professionals to spend a year on rotation fully away from the IC embedded with a technology organization, with the IIB and In-Q-Tel helping facilitate placement (R63). Additionally, IC organizations should at a minimum loosen restrictions and, ideally, actively encourage officers to take "leave without pay" (LWOP) to pursue paid opportunities in the technology sector while maintaining their eligibility and clearance status to return to the IC.

- The ODNI should also establish a complementary Innovator in Residence program, selecting 8 to 10 private sector technologists and entrepreneurs with interest or experience providing tech to the IC to embed in IC organizations (R64). Depending on clearance levels, innovators could be placed in IC research organizations such as IARPA or CIA Labs or be embedded in mission directorates and centers. To attract talent, the IC should lift the lifetime publication review requirement for Innovators in Residence and instead require review only on topics pertaining directly to their work in the IC and for a limited number of years.

Public-Private Partnerships: The benefits of IC-private sector collaboration—from innovation to algorithms to analysis—to both the IC mission and commercial partners could perhaps be best tested and demonstrated through jointly attacking one issue or threat critical to the United States through a public-private partnership.

- The IC should establish a **biotechnology public-private partnership** with U.S. commercial biotechnology firms and other biotech research organizations willing and able to share data, insights, and analysis of emerging biotechnologies and applications with implications for U.S. national security (R65).

Research Community

In addition to the commercial sector, the U.S. research community—to include national laboratories, FFRDCs, University Affiliated Research Centers (UARCs), and academic institutions—will often be at the leading edge of development and experimentation of technology with IC applications. While still sponsoring classified research, the S&T and advanced research portion of the IC must be integrated into the day-to-day research, testing, training, and collaboration on AI and associated technologies that occurs primarily in the open-source domain. IARPA funds many of these organizations, and CIA Labs is also building what should be deeper cooperation with national labs, universities, and other research organizations on shared technology challenges and opportunities.

ACADEMIC INSTITUTIONS

U.S. leading universities are engaged in frontier research creating future game-changing possibilities and scientific breakthroughs. This cutting-edge research could and should be harnessed by the IC before it becomes more widely available in the venture capital or commercial ecosystems.

- IC R&D entities such as CIA Labs and IARPA should expand efforts with U.S. universities to collaborate and sponsor research, development, testing, and engineering of S&T solutions for intelligence problems, particularly in the AI space (R66). IC organizations should focus on identifying unclassified problems that are analogous to classified ones to enable uncleared university researchers to contribute to research that still has mission application.[70]

In addition to capturing research expertise, the IC must also build bridges to U.S. universities to attract, recruit, and retain the next generation of tech leaders. As part of a new talent acquisition and management strategy (as detailed in the "Workforce" section), the IC must build a **next generation talent pipeline** to U.S. universities. A sustained program of outreach and opportunities for university students to get involved with the IC will be vital in helping them understand the various ways they could serve the IC mission, whether inside the community or from the private sector. Many top STEM students are simply not aware of IC roles and, if they are, are only approached when nearing graduation and likely weighing more lucrative and speedier offers from tech firms. An IC talent pipeline strategy could incorporate several steps:

- The IC should establish robust, on-campus academic outreach offices that include intelligence officers in residence and university fellowships, guest speaker series, and online lectures on intelligence topics (R67).
- The IC should increase the number of IC summer internship programs for college STEM majors after their freshman year (R68). This is a major window of opportunity, since few major tech companies hire engineering students that early.
- The IC should build upon the DOD's Hacking for Defense program with IC-centric versions focused on real-world, policy-relevant intelligence problems (R69). The ODNI could publish unclassified research topics with secure portals and digital resources for students to research and collaborate.
- The ODNI should create a high-profile IC fellowship program for 25 to 50 graduating STEM students from top universities (R70). Led by the Intelligence Innovation Board and supported by IC agencies and commercial sector partners, fellows would be trained as a cohort and placed in diverse IC organizations to work and collaborate on a hard IC problem for one year before starting graduate school or their tech career. The goal of the program would not be to develop career civil servants but rather to have talented young STEM experts take a formative IC experience with them as they move into research or the private sector—building a virtuous cycle in the IC-private sector-research ecosystem over the longer term.

NATIONAL LABS AND RESEARCH CENTERS

The IC must harness the expertise and ability of national laboratories, FFRDCs, and UARCs to work on both classified and unclassified problems and conduct mission-focused research on technologies with IC applications, in both the near and long term. These research organizations have particularly strong expertise in AI and should be leveraged to develop, test, and train algorithms and models for IC use.

IC agencies should create formal AI partnerships with the research sector (R71). These partnerships could include:

- Verifying and validating algorithms, performing testing and evaluation (T&E) on IC models, and collaborating on new AI application methodologies;
- Coordinating to identify data sets for researchers to train on and creating rubrics for scoring and testing; and
- Creating joint competitions such as an unclassified AI Olympics to generate ideas for solving real IC problems with analogous data sets and interest from early-stage researchers in priority areas, particularly if grant or prize funding is attached.

Foreign Allies and Partners

As the U.S. IC adopts the best tools and technologies from the commercial and research sectors, it must also deepen and expand its relationships with allied and partner foreign intelligence services at the cutting edge of intelligence innovation. Beyond traditional intelligence sharing and liaison partnerships, the U.S. IC must reconceptualize and adapt how it develops, employs, and exploits emerging technologies with partners at the innovation edge. With common enemies, shared threats, and differing areas of innovation strength, the United States must leverage the technology-enabled intelligence capabilities with like-minded partners, including the Five-Eyes (FVEY) alliance, NATO, Israel, and allies in Asia.

In short, U.S. intelligence must reimagine its closest liaison partnerships from ones centered on intelligence **sharing** to ones of intelligence **generation**, building a full-spectrum intelligence partnership that jointly develops technology and executes tech-enabled intelligence missions.

Joint Innovation: U.S. intelligence must synchronize its major technology investments, AI product and application development, and strategic R&D with allies and partners. Common digital infrastructure, talent pools, and engagement with the commercial sector will enable U.S. intelligence to tap into expertise and technology from trusted partners around the globe.

- The ODNI should lead interagency efforts to build a **FVEY cloud** as the basis for technological collaboration and intelligence generation with its closest intelligence allies (R72). A FVEY cloud would serve not only as the primary platform for data and intelligence sharing but also as shared common foundation for algorithm and application development and joint deployment of AI to enable missions and workflows worldwide.

- IC agencies should support **AI talent exchanges**, sponsoring S&T analysts, data scientists, engineers, and researchers to spend one to two years embedded in foreign partner organizations working on joint intelligence innovation (R73). The IC could start with pilots with FVEY allies and look to expand to other like-minded partners.

- The ODNI should invite FVEY agency and commercial sector participation in the IIB to build common understanding of emerging technology trends and foster joint strategic partnerships with industry (R74).

Fielding, Collection, and Operations: U.S. and foreign partner agencies must leverage each other's strengths in collection, including access and proximity to priority targets, technical platforms, and AI fielding, and integrate emerging tech into joint tradecraft and operations, particularly on hard targets such as China and Russia.

- IC collection agencies should develop and implement a **Joint Tradecraft Initiative** with select allies and partners—multilaterally or bilaterally—to envision and develop new collection tradecraft harnessing emerging technologies (R75). DNI representatives in the foreign field should be given the training, resources, and authorities to oversee and execute the initiative in the field with support from headquarter agencies.

Algorithm and Data Set Sharing: In addition to joint tradecraft and operations, the United States and like-minded partners should also collaborate on sharing algorithms, models, and data sets, especially where partners have particular strength in data and expertise, such as Australia on China or Baltic and Nordic allies on Russia.

- The ODNI and USDI&S, working with its commonwealth allies, should harness a FVEY cloud for an Allied Algorithm Project, building common data lakes to collaborate on training, testing, validating, and employing algorithms for common intelligence and defense mission applications (R76).

Real-Time Intelligence Sharing: Intelligence sharing between allies and partners is often slowed due to antiquated and tedious release, redaction, and dissemination policies and processes. AI tools could be developed to automate and expedite intelligence sharing and enable allies to share important and time-sensitive intelligence closer to real time.

- The ODNI CTO should sponsor an Automated Tearline Project that uses AI to develop rapid, automated intelligence sanitization and dissemination applications for use with allies and partners (R77).

Joint Products and Distribution: Analysts should harness a FVEY cloud to collaborate on joint analytic products that harness AI, analytics, and other technologies and deliver them to allied customers.

- The OSC should take the lead in developing a weekly OSINT analytic product generated jointly with FVEY allies, exploiting AI and data analytics for timely analysis on a particular global issue or trend conducive to these tools, such as foreign S&T development or regional instability indicators and warning (R78).

STRATEGIC R&D AND NEXT GENERATION TECHNOLOGIES

While the commercial sector, research community, and foreign partners will produce many technologies that meet IC needs, particularly in AI, the IC must also accelerate its own R&D efforts in areas unique or acute to the IC. Throughout the history of the IC, it has been researchers funded by institutions such as IARPA and the Defense Acquisition Research Projects Agency (DARPA) that have created technologies that have changed what is possible for intelligence missions. Those organizations, particularly IARPA for the IC, must be empowered—and funded—to innovate and find the next generation of technologies and applications that will help deliver strategic intelligence advantage.

Leap-Ahead Technologies: The task force focused primarily on near-term applications of advanced technologies, but the study has made clear the vital importance of IC innovation for the next generation of technologies that will disrupt and transform intelligence missions. While no single technology will be decisive, the IC must begin strategically planning how it will develop and integrate

technology in the following fields.

- **Biotechnology:** Rapid advances in biotechnology have the potential to substantially improve human health and environmental quality but can also pose grave risks. The persistence of biological weapons programs, along with the possibility of catastrophic laboratory accidents, will place new responsibilities on the IC to detect, analyze, and attribute disease outbreaks and other biological events. For the IC, biotechnology could also alter the very nature of intelligence collection and spawn a new field of bio-intelligence. Converging advances in synthetic biology, AI, and computational power could create transformational new collection capabilities in biosensing, biological geolocation, and DNA data storage and transfer.[71] While providing a strategic intelligence advantage, bio-intelligence will also pose profound ethical questions for IC leaders.

- **Quantum:** Advances in quantum sensing, computing, and networking will likely transform many collection, processing, and analysis missions. The race for quantum encryption and decryption could determine the future of SIGINT and the IC's ability to collect and secure intelligence assets, access, and data. Beyond cryptological implications, quantum technology could accelerate many of the AI/ML applications and capabilities identified in this report.

- **5G and Intelligence IoT:** The mass fielding of 5G and IoT devices augurs dramatic shifts in where, what, and how intelligence is collected, creating opportunities for collectors but exponentially growing burden for processing. Ubiquitous connectivity, disconnection of hardware, and edge computing could enable intelligence to be generated almost anywhere at 5G speed. At the same time, the volume and variety of 5G data and the number of signals and emitters from IoT devices will further inundate the IC with data to sense, process, and synthesize.

- **Space:** While harnessing commercial satellite collection services, the IC must develop and harness next-generation space capabilities for long-term sensitive collection needs. On-orbit service, assembly, and manufacturing (OSAM); hyper-spectral sensors and large apertures; and large numbers of cheaper, smaller satellites with onboard updating will be vital for IC needs.

The IC must prioritize strategic R&D and the application of these "leap-ahead" technologies to gain a decisive technological-intelligence advantage—namely over China—in the decades ahead. While some of these technologies could be developed in-house, others will require investment in non-IC strategic partners. And given the scale, complexity, scope, and potential impact of these investments, they must be coordinated across IC agencies and be able to adapt to inevitable shifts in technology with intelligence implications.

- The DNI should consider further empowering the ODNI Office of Science and Technology and elevating its director to serve as the U.S. IC chief technology officer (CTO) (R79).

- The IC, with congressional support, should create a **Technology Investment Fund** administered by the ODNI and IC CTO focused on developing new IC-specific capabilities and providing multiyear flexibility to meet agile acquirements (R80). The fund should focus on the above "leap-ahead" technologies as well as IC-centric versions of other technologies such as AI that are tailored for sensitive collection, processing, and analysis missions. The ODNI fund should make use of prize challenges, Other Transactions, and other alternatives to traditional technology procurement and ensure investments are coordinated with those of individual IC agencies.

"Blue versus Red" Technology Strategies: Advantage in future technological-intelligence environments will be an iterative competition in which adversaries "get a vote." Strategic R&D and future technology investments will require not only accurate forecasts of technological trends and but also assessments of adversary strategy, capabilities, and intentions in integrating technologies into intelligence operations. Integrated intelligence support from S&T and country-specific experts will be critical in correctly steering strategic R&D and investments.

- In addition to regular intelligence support to IARPA, DARPA, and other U.S. government advanced research agencies, the ODNI should leverage its new IC Net Assessment Office to conduct an annual **Technology Net Assessment** of U.S. and key adversary technology strategies, future capabilities, and potential countermoves to U.S. investments (R81).

Mission Integration and Transition: Building better connections between research and application will be essential to ensure IC-developed technologies are adopted

"The IC must prioritize strategic R&D and the application of these "leap-ahead" technologies to gain a decisive technological-intelligence advantage—namely over China—in the decades ahead."

into IC missions. The technology end user—collector, analyst, and S&T targeter—must have a seat at the table from the beginning of R&D efforts to help map the capability to the real-world problem set and throughout the project life cycle to help researchers adapt to changing missions, priorities, and operating environments.[72]

- ODNI S&T and IARPA should conduct annual roadshows to IC operational and analytic directorates and mission centers to educate and demonstrate to users the latest emerging tech with potential mission applications (R82).
- Going the other direction, directorates and missions should sponsor and incentivize collectors and analysts, particularly those with foreign S&T specializations, for rotational opportunities at IARPA to gain firsthand experience with innovation (R83).

Basic Research: In addition to mission and application-focused R&D, basic research for scientific exploration will still be essential for discovering future game-changing IC capabilities that may not yet be imaginable. Ensuring IARPA and other IC R&D centers have stable, secure, and long-term funding for research that may take a decade to show operational viability must be a priority.

- The IC and Congress should work together to set aside secure and significant funding for basic research and fundamental scientific exploration. Congress must protect those budgets from being harvested for operational and maintenance budget shortfalls while ensuring the research is in line with broad intelligence and national security priorities (R84).

Secret and Unclassified Work: Much of the research for even the most cutting-edge technologies for the IC can be done at the secret or even unclassified level. Yet too many would-be IC researchers are left waiting for TS/SCI clearances they do not actually need, leaving no choice but to opt out of the hiring process. Expanding and expediting the number of non-SCI positions at IARPA and IC research organizations will be vital for the IC's ability to attract world-class researchers, broaden and diversify its talent base, and enable faster turnover of staff—natural in the S&T world—at the pace of technological change.

- IC research and S&T organizations should set aside a certain percentage of total billets—perhaps starting at 10 percent and gradually increasing—that only require secret clearances and collaborate with commercial and research sector partners to identify project roles that require no clearance at all (R85).
- The ODNI, using the IIB and partnerships with academic and national labs, should explore the creation of the Tech-Intel Reserve Corps. Like military reserve units, these tech experts could conduct annual exercises and provide monthly research support to IC agencies on secret or open-source research projects while receiving IC training and compensation (R86).

INFRASTRUCTURE, ARCHITECTURE, AND SECURITY AND ASSURANCE

The IC cannot harness the potential of AI and associated technologies for intelligence advantage if it lacks agile and adaptive digital infrastructure, more open and collaborative data architecture, and data and systems that are secure and assured. The IC has largely succeeded in its first major step toward IT modernization with the adoption of cloud computing. But proliferating and diversifying global threats and shifting mission priorities will require more flexibility, interoperability, resiliency, and creativity in where and how data and intelligence is shared, accessed, stored, and actioned to meet operational needs.

Infrastructure

Robust enterprise IT and computing infrastructure will serve as the backbone of day-to-day IC operations and the digital

foundation on which AI and associated technologies can be applied and integrated into intelligence missions. The IC has already laid the groundwork through Commercial Cloud Services (C2S) and the transition to cloud computing. The next step will be building upon this success to create the next generation of digital infrastructure capabilities to meet future mission needs. The task force seconds many of the initiatives and recommendations outlined in the ODNI's 2019 cloud computing strategy but offers a few specific areas of focus based on research.[73]

Multilayer Fabric: A multilayer cloud infrastructure that is diversified yet interoperable will be vital in enabling diverse workflows within and across networks that are flexible and resilient enough to allow users access from wherever the mission requires. Secure and deployable IT with global reach is vital, but part of that reach must include a secure cloud at the unclassified level. The IC has never invested significantly in unclassified digital infrastructure. But as emphasized throughout this report, to harness AI and build the necessary strategic partnerships, the IC must be able to communicate and operate in open-source and remote environments. The strategic necessity of secure, remote, and unclassified work has been made abundantly clear through the Covid-19 pandemic.

- In conjunction with IC agencies, **the ODNI should conduct a comprehensive Covid-19 remote work review** of what has been achieved through the pandemic, an assessment of risks and benefits, and a collection of lessons learned and recommendations for the future of IC remote work (R87).

Edge Cloud: The IC's global cloud capabilities must be available to users at the edge of IC networks. This includes commercial and unclassified environments and, perhaps most critically, collectors operating in forward, remote, and contested intelligence operating environments. Many of the opportunities and recommendations outlined in the "Collection" section of this report will require cloud capabilities for edge users in disconnected, degraded, or high-threat areas and the ability to have secure access to data, AI, and computing power at the time and place of mission need.

- IC infrastructure and technology leaders should collaborate with operational agencies and directorates to prioritize building **forward-deployed cloud**, focused on delivering secure, resilient, rapidly deployed cloud services and AI applications to operators at the edge (R88).

Scaling: The IC must ensure that its digital infrastructure is conducive to scale and that all parts of the mission can leverage the services, benefits, and efficiencies of cloud and cloud-enabled software technologies, particularly AI/ML. Any cloud strategy must be enterprise-wide to enable dispersed users to exploit the advantages over the long term. It must also account for the fact that not all users need access to tools, platforms, and computing power in the cloud all of the time.

The IC should build on the IC Information Technology Enterprise (ITE) and C2S toward an interagency **IC Cloud** (R89). An IC-wide cloud would enable greater AI interoperability across the community and could have several core attributes that facilitate scaling AI, including:

- A cloud-enabled AI-platform, similar to the DOD's Joint Common Foundation, that enables enterprise access to AI tools and data and synchronization of AI projects across agencies and puts out algorithms for community usage and adaptation;
- A secure environment in accordance with development, security, and operations (DevSecOps) best practices and principles;
- Software accreditation for IC-wide usage, not just by individual organizations; and
- A consumption-based "utilities" model for cloud computing usage, based on time and power used in the cloud, to generate cost savings and efficiencies.

Architecture

This report details the many transformative applications of emerging technologies such as AI/ML, but they are nothing without high-quality data to train and power those applications and a data architecture that enables user access to data. The adoption of an enterprise cloud should enable the IC to transition away from the closed data architectures of the past to more open architectures conducive to the speed and ease with which data much be stored, transferred, shared, and accessed for mission impact.[74] The transition will not be simple, given legacy processes and legitimate risks to security, but the IC can and should move expeditiously to enable data and cloud-native capabilities to be accessible to users regardless of platform.[75]

"... to harness AI and build the necessary strategic partnerships, the IC must be able to communicate and operate in open-source and remote environment."

Conditioned Data: The IC has an overwhelming abundance of data. What the IC still lacks is conditioned data suitable for training on the scale needed for IC-wide applications.[76] Data sets must be large, high-quality, representative, and consistently tagged—a tedious, time-consuming, and still primarily human task exacerbated by differing labeling standards across and even within agencies.[77] Unlike the private sector, which can crowdsource and employ gig economy taggers, the IC's classified data sets require that labeling 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.[78]

- The recently established IC chief data officer should work with the IC CIO to develop common data conditioning, tagging, and labeling standards, including for metadata, that will facilitate cross-IC usage and application (R90).
- The IC should invest in **synthetic data** (and associated storage and computing power) both to expand the number and size of training data sets and reduce the time and burden of human analysts doing labeling (R91). Since users are creating synthetic data, it can be labeled from the beginning of the process. Training AI models on synthetic data could also help increase accuracy while still enabling users to apply the models to real-world data.

Removing Stovepipes and Silos: Large-scale, high-quality, and consistently tagged data sets are mission-critical assets but cannot be turned into insights and action if they cannot be shared or accessed. Inside the IC, vital data often remains hidden in silos buried across IC organizations and on incompatible and inaccessible data architectures with varying data governance and access standards that prevent sharing and collaboration.[79] Closed data architecture also hampers IC integration with commercial providers, lacking known, open, and unclassified interfaces to effectively integrate data sets, algorithms, and software.

- The IC chief data officer should spearhead an interagency initiative to assemble large-scale classified training data sets available to any IC agency, with data conditioned according to the standards framework described above (R92).
- The PDDNI should also push for individual agency CIOs and data managers to identify ways to reduce barriers to entry and promote data sharing and AI interoperability through open architecture and more flexible access authorities (R93).

Multi-INT, Cross-Domain: The ideal IC data architecture for AI applications would be able to integrate data in at least two ways. First, it would curate and merge data from multiple "INTs" into common data lakes that allow algorithms to analyze patterns across data sets, automating the ability to "tip and queue" platforms for new collection. Second, it would be able to fuse both classified and OSINT data into training and deploying these algorithms.

The technical, security, and policy challenges of both "multi-INT" and "cross-domain" data architecture are undoubtedly large. The rich variety of data of interest to analysts—structured and unstructured text, sensor or human-derived pixels or text—will be hard to standardize for AI training and development, while incompatible architectures and security barriers will likely hamper "low-side"/"high-side" integration. Nonetheless, the potential of harnessing all data—from any INT, at any classification—would be a true game-changer and leap-ahead capability for the IC, widening the data aperture, sharpening what is surfaced, and accelerating synthesizing and action.

- The ODNI, with agency CIOs and S&T directorates, should launch a **cross-domain challenge** to test the feasibility of building and training IC-specific algorithms and models on multi-INT data and both classified and open sources (R94). This initiative would likely require the support of IC strategic partners, including in the commercial sector and national labs with supercomputer and other world-class capabilities. While exploring the technical feasibility, the ODNI should also move to institute the necessary IC policy

changes.

Security and Assurance

As U.S. strategic competitors accelerate adoption of AI into military and intelligence operations, the U.S. IC will face persistent, aggressive, and targeted cyberattacks and adversarial AI efforts aimed at penetrating and undermining the capability of and trust in AI systems. The IC's urgency to adopt AI cannot come at the expense of rigorous AI security standards, protocols, and testing requirements. Doing so would create critical vulnerabilities to a range of "counter-AI" threats, from "poisoned" data injected into AI models to fully hacked and manipulated systems.[80] Even if adversaries cannot gain such a level of access, convincing collectors and analysts their AI is compromised and unusable could achieve the same effect.[81]

Security: The IC's response to security and adversarial AI threats cannot be retrenchment from rapid technology acquisition and adoption. Rather, cutting-edge security technologies and testing, evaluation, verification, and validation (TEVV) best practices must be integrated into the procurement, investment, and assimilation of AI and associated hardware, software, and platforms from start to finish and continually after to facilitate security, accountability, and trust.

- IC agencies should prioritize **investment in emerging security technologies**, to include AI-enabled cyber defense, advanced cryptography, countering adversarial AI, threat intelligence/anomaly detection, and supply chain security (R95).
- IC agencies should adopt best practices in DevSecOps for software development and deployment, including from the private sector and innovators in the DOD, such as the Joint Artificial Intelligence Center (JAIC) (R96).
- The ODNI, in partnership with the DOD, should establish a **National AI/ML Red-Teaming Center** with focus on simulating and testing AI systems against adversarial AI (R97).[82] The center would be independent, staffed with technical and country expertise to simulate realistic adversary attacks, and build upon existing efforts, such as Hack the Pentagon cyber exercises and ongoing efforts of NSA R6.

Testing and Evaluation: AI systems are unique in that the systems learn over time. This learning is based on the inputs and environments the systems are exposed to and the rulesets established during training. Once in operation, the AI system can drift, exhibit biases, or produce unexpected outputs. To build IC confidence in AI systems will require research in and development of capabilities that provide model explainability and auditability; stress-testing and understanding of failure modes; and, ultimately, an ability to continuously monitor the operational performance of the AI system and determine when model retraining is necessary. The IC can also collaborate with the DOD, academia, and private sector to develop and mature an ecosystem centered around AI test and evaluation, including methods, processes, and capabilities.

- In addition to red-teaming, the ODNI and IC agencies should adopt TEVV best practices and standards, leveraging its strategic partnerships with the private sector, research community, and foreign allies for lessons learned (R98).[83]

Assurance: Analysts have always been responsible for verifying sources of intelligence or inputs into analytic thinking, but they now must be able to measure a new factor once taken for granted: the authenticity of the data. Ensuring data and intelligence authenticity will only grow harder as the scale, sophistication, and complexity of adversary disinformation and digital manipulation efforts grow more persistent and aggressive. The challenge grows even more critical as the IC opens its aperture—as this report recommends—to include more sources of information that it does not control.

Legacy processes and cultures of risk avoidance will likely tempt some IC organizations to evade tackling intelligence assurance challenges simply by not allowing data collected from outside the IC with unknown pedigree and provenance. Rather than risk **avoidance**, the IC must adopt a risk **management** posture, which would be an enduring process of exploring, documenting, and protecting the pedigree of the information flowing into IC systems and thinking.

- IC agencies should explore historic assurance models, including the NSA's Information Assurance mission and the NGA's recently built Office of GEOINT Assurance, to identify best practices (R99).

ETHICS AND GOVERNANCE

Harnessing AI will require intelligence

users to understand the impact and outcomes of applying AI in intelligence processes and missions. It will also require policymakers, congressional oversight, and strategic partners to understand how the IC is applying AI and doing so in an ethical manner. The ODNI's "Principles of AI Ethics for the Intelligence Community" establishes a clear framework and guidance for how IC agencies can develop and use AI in accordance with legal obligations, establish norms and principles, and ensure IC users build, procure, and use AI ethically, responsibly, effectively, and usefully.[84] Indeed, the rush to adopt and harness AI may lead IC agencies to jump over the first order question: why use AI in the first place, and why will it be more effective in meeting the mission need than other means and methods?

When the IC does choose to develop and exploit AI, clear and consistent application of ethics, governance, accountability, and transparency will be essential throughout the AI life cycle. Transparency, in particular, will be vital in how the IC communicates its AI needs and requirements to the U.S. commercial and research sectors, which the IC will need for AI innovation. While some U.S. innovation firms will simply not want to partner with the IC for various reasons, transparency in AI principles and ethical conduct will help enable the private sector to make more informed decisions on supplying technology to the IC and to communicating and justifying these decisions to their own workforces.

Privacy and Civil Liberties: The incorporation of OSINT and PAI into IC analysis raises not only security problems but also compliance issues, with legal and policy requirements, data governance, and ethical concerns regarding U.S. person information. As noted throughout this report, the IC must be able to continually surface and synthesize open-source data, but the broad groomings and queries of data sets of value and interest could run afoul of rule sets that seek to ensure the right to privacy and protections of civil liberties.[85] The policy, architecture, and infrastructure of search, storage, and access of U.S. person data, however, is based on assumptions and specific types of targeted searches more applicable to previous decades and not for broad discovery and sensemaking of big data.[86]

- The ODNI Office of Civil Liberties, Privacy, and Transparency, in conjunction with relevant National Intelligence Managers, S&T directorates, and CIOs, should launch an **Open Source and Civil Liberties Initiative (R100)**. It would aim to find solutions to enable IC agencies to access OSINT and PAI data that may include information derived from U.S. persons, identify what legal and policy requirements necessitate updating, and ensure those requirements are consistent with respect for individual rights and liberties of affected individuals.

Explainability and Transparency: As analysts, collectors, and policymakers begin using AI-derived findings, they will require knowing the logic, bias, assumptions, and inferences of 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 "blackbox" algorithms in which machine logic and processes are hard if not impossible to define. Lack of transparency on evidence chains, where and how AI was used, and validity conditions means machine findings could be untrustworthy and unusable.[87]

- IC agencies should collaborate to determine **common standards and best practices for AI explainability in AI enabled workflows and analytic products**, to include how certain types of algorithms should or should not be applied and how to clearly explain AI application and implications in intelligence products (R101). IC explainability practices should conform not only to analytic tradecraft and review standards but also to IC responsibilities for transparency and accountability in its work for policymakers, Congress, and the public.[88]

- IC agencies should also leverage strategic partnerships with the private and research sectors for ideas and best practices on transparency and explainability in AI-enabled workflows, such as use of model cards for AI and ML models (R102).[89]

Bias and Judgment: Generating insights from AI requires analysts selecting certain data sets and helping to shape, hone, and steer algorithms and models. But analysts introduce bias in how they conceptualize the intelligence problem, design the model, and select and label 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 be easily understood by customers.[90] AI users in the IC must be able to recognize, account for, and mitigate bias to the extent possible without reducing the model's utility.[91] Moreover, the inherent risk of data and algorithmic bias means that data scientists

and analysts must be "in the loop" of AI applications, particularly those meant to inform critical policy and operational decisionmaking, until IC users have verified and validated confidence in the model.

- The ODNI Office of Mission Integration should gather an inter-IC working group to develop best practices for understanding, documenting, mitigating, and communicating AI bias in AI-enabled workflows and products (R103).

CROSS-CUTTING THEMES AND CONCLUSION

The Need for Reinvention

While conducting research to identify the applications of emerging technologies for intelligence missions and the enablers that must be put in place to seize those opportunities, the CSIS Technology and Intelligence Task Force also uncovered several key, overlapping themes that permeated its discussions and study on how to implement change. The word and idea that connects these themes is **reinvention**. The emergence of AI, big data, and other transformative technologies must compel the IC to reinvent how it conceives, prioritizes, and executes its missions; how it builds strategic partnerships and stakeholder buy-in; and how it wins and retains the strategic advantage over its adversaries and in serving its customers. How can the IC pursue this intelligence reinvention?

Leadership: Reinvention must start at the top and will require committed leadership across IC agencies to drive these changes through the bureaucracy, find the obstacles, and solve them. Senior leaders, in turn, must empower leaders at the directorate, mission center, and even team level to seize the opportunities of innovation for mission gain and incentivize creativity, speed, and experimentation in how technologies are integrated and applied. Investment of time, training, and education of senior and mid-grade IC managers in understanding the capabilities of emerging technologies to assist intelligence missions can help reduce their reluctance to embrace these technologies and change perspectives and attitudes on intelligence innovation.

Culture: As noted to the task force on several occasions, "the IC does not have a technology problem; it has a culture problem." Perhaps the biggest innovation the IC needs is not technology; it is how to change IC culture to be more open to technology. The IC's culture of acquiring and adopting new technologies remains **compliance-centric**—checking every box of bureaucratic and programmatic protocol—rather than **mission-** and **customer-centric** in enabling intelligence missions and users. Cultural change will take time but will occur with the right mix of people: the next generation of digital natives, top-level leaders who believe and inspire, and managers, mission centers, and senior analysts across the bureaucracy who can be "innovation early adopters" and help change the culture from within. Change can—and must—be accelerated through the clear and rapid demonstration of technology's mission value to resistant organizations and cultures, including through many of the mission-centric applications of technology highlighted in this report.

Risk: When it comes to technology adoption, IC decisionmaking remains too focused on the risk of **action** but fails to assess and incorporate the risk of **inaction** and the opportunity cost of not acquiring and integrating new technologies into intelligence missions. This task force does not cavalierly dismiss the critical threats and risks—in cyber, adversarial AI, and CI—associated with new technology and data streams. Indeed, risk must always be central in analyzing technology adoption, but decisions cannot be made solely on those grounds. An element of IC culture that leaders must prioritize transforming is this risk aversion, where risk-taking, experimentation, and creation will be rewarded and where innovators are not unduly punished when there is inevitable failure. In fact, IC leaders can look to a core part of the IC enterprise as an example of a mission that already accepts and integrates risk into decisionmaking—the CIA Directorate of Operations (DO), which balances rigorous monitoring of security and CI with bold and creative approaches to mission execution. The rest of the IC could do so as well.

Agility and Adaptation: No single technology or set of emerging technologies will decisively deliver mission success and intelligence advantage to the IC, nor will any advantage be long sustained, given rapid shifts in new technologies, the likelihood of technological surprise, and innovative adversarial approaches. Rather, what will likely be decisive is the **creativity** and **commitment** of IC leaders and organizations to integrating and harnessing new technology, and the **speed** and **urgency** at which the IC adapts to technological change. Such IC agility and adaptation cannot be achieved alone and will require support from the IC's strategic partners, particularly in the U.S. commercial sector. Incubators such as SOFWERX and AFWERX can serve as the models for IC-private sector integration in better linking IC users to those developing the capabilities, facilitating more rapid adoption. In addition to cutting-edge technology, U.S. innovators can also provide the IC the best practices for how to evolve its organizational processes, risk culture, and business models to prioritize innovation and change instead of the status quo.

Policymaker Support: The IC will face a dizzying array of conventional, unconventional, and unforeseeable threats to U.S. national security. However, the necessary trade-offs among the range of daunting security and intelligence challenges that confront the United States are the responsibility of elected and appointed officeholders and not the IC. The importance of clearly stated requirements from U.S. policymakers will increase as the volume of data

grows. The IC will simply be unable to separate "wheat from chaff" without strategic priorities against which collectors and analysts can smartly and efficiently target their efforts. U.S. policymakers can further assist the IC and its leaders seeking to innovate by making technology adoption a top priority for national security. Customers should send a clear demand signal for intelligence products that incorporate AI, big data, and other cutting-edge technologies into their analysis and delivery. If the IC cannot incentivize AI adoption, its senior-most customers can.

Oversight and Transparency: IC reinvention will not entail small tweaks to the system, marginal reform of organizations, or building slowly on already tepid progress. It will require wholescale change to organizations, missions, and personnel and to the associated authorities, policies, and budgets needed to execute reinvention. Change on this scale will require partnership with the IC's overseers in Congress. Engagement with Congress must be early and continual to ensure buy-in and the necessary flexibility in budgets and programs to adapt to inevitable and unanticipated shifts in emerging technologies and intelligence priorities.

The overarching conclusion of this Technology and Intelligence Task Force is two-fold. First, technology itself is not the obstacle for IC reinvention, as there is no shortage of emerging technologies that can be directly applied to IC missions or of commercial partners willing to provide those technologies. Second, what is an obstacle—and perhaps the decisive one—is cultural resistance to risk and change and with it an incentive structure that prioritizes non-failure and standard approaches over risk-taking and innovation. The obstacle of culture must and can be overcome—through inspiring and demanding leaders; a vibrant, diverse, and digitally-savvy workforce; and the support of stakeholders in policy organizations, Congress, industry, the research community, and foreign capitals.

The U.S. IC faces perhaps the most serious and rapidly accelerating set of threats in its history. From strategic rivals China and Russia to global terrorist and extremist movements to cyber and information warfare to, as the Covid-19 pandemic has shown, global health and new biothreats, the IC must not only anticipate and accurately assess this threat landscape but also do so in a manner that clearly and demonstrably justifies its cost and value-added to U.S. policy. The integration of emerging technologies will play perhaps the deciding role in the IC's ability to execute these missions. The IC must begin now to **reinvent** its culture, priorities, processes, workforce, and the relationships with its vital stakeholders: the policymakers it serves, the strategic partners who provide it with technology, the congressional members and committees who oversee it, and ultimately the American people.

APPENDIX A: TASK FORCE SCOPE AND METHODOLOGY

This appendix sets forth the concept, research design, methodology, and scope for the Center for Strategic and International Studies (CSIS) Technology and Intelligence Task Force.

Background

Maintaining a competitive edge in strategic intelligence over increasingly sophisticated rivals and adversaries will be a critical component of ensuring and advancing U.S. national security interests in the coming decades. While many scholars have written on the implications of rapid technological advancements for the future of warfare, CSIS identified a gap in current scholarship on the specific implications for U.S. intelligence, at least at the unclassified level.

The Project

CSIS assembled a task force to undertake a 12-month project exploring how emerging and advanced technologies such as artificial intelligence (AI), machine learning (ML), cloud computing, and data analytics can be applied and integrated into the operations of the IC. The task force was designed to comprise a cross-section of key leaders and world-leading experts from the tech, intelligence, policy, and research communities with a passion for advancing the U.S. intelligence mission through technological change. The core deliverable of the task force was a series of assessments and final report on how the IC must evolve through innovation in order to remain the global gold standard in strategic intelligence and serve U.S. policymakers.

Objective

The goal of the task force is to generate an action plan for key public and private stakeholders to change, improve, expand, and accelerate the ways in which advanced technology is used to produce strategic, national-level intelligence for senior U.S. policymakers. Specifically, the task force sought to identify technical, process, policy, and legislative solutions to ensure American technology will better enable the **collection**, **analysis**, and **distribution** of high-impact intelligence to policymakers. Under this overarching project goal are three other key objectives:

- **Convening Stakeholders:** CSIS will bring together the right mix of experts from across the intelligence, policy, technology, research, and legislative communities to build shared understanding of the technology, the intelligence process, and how to implement change.
- **Actionable Research:** Task force participants will put themselves (back) into the seats of collectors, analysts, and policymakers to generate creative but practical ideas and help the CSIS research team craft rigorous but solutions-focused research products.

- **Future Community of Interest:** Beyond the project year, CSIS aims for the task force to be an enduring community of experts and collaborators committed to maintaining America's intelligence edge while innovating new ideas for continuing research.

Scope

Given the scale of the issue of technology and intelligence, the task force could not investigate all of the emerging technologies with potential intelligence applications, nor all types of intelligence analysis and intelligence missions that could benefit from innovation. The task force scoped its research to the following areas:

- **Technologies:** The task force focused on the implications of AI/ML, cloud computing, multimodal sensors, and advanced data analytics. These technologies were chosen because of their near-term, direct application to intelligence missions and their interdependence in intelligence systems, processes, and products. Other technologies, such as space-based collection, additive manufacturing, quantum systems, 5G networks, robotics, miniaturization and nanotechnologies, and synthetic biology, will also transform the IC. These technologies are touched upon in the report but are not the primary focus.

- **Missions:** From an intelligence mission perspective, the primary focus of the task force was on the **collection**, **analysis**, and **distribution** of intelligence. Other critical mission areas, including counterintelligence and covert action, are briefly discussed in the report.

- **Products:** From an intelligence product perspective, the task force focused on strategic, national-level, all-source intelligence intended for U.S. policymakers. The report assesses technology's benefits for operational and tactical-level intelligence but in the context of it informing strategic analysis and national-level intelligence missions.

Research Question

The overarching research question for the task force is: what are the opportunities and obstacles to integrating advanced technologies into the generation of strategic intelligence, and what actions must the IC and its key stakeholders—policymakers, Congress, the technology and industrial sectors, and the research community—take to ensure future advantage?

The key related questions answered throughout the project year include:

- How is the IC exploiting emerging technologies to improve intelligence collection across the various means of collection—human, signals, imagery, and open-source? What emerging tech is most relevant and impactful for each means of collection?

- For all-source analysts, what aspects of data collection, sorting, and analytic tasks can be improved, accelerated, or offloaded through AI/ML, cloud computing, and analytics?

- How can "analyst-machine" performance be optimized to maximize data intake, streamline processing, prioritize relevant information, and create more bandwidth for analysts to think and write strategically?
- How can emerging tech such as AI and cloud be used to improve collaboration, coordination, and review of intelligence products, and optimize their dissemination to policy, intel, and military consumers?
- What are the implications of success and failure to harness emerging technologies into the U.S. intelligence enterprise for U.S. national security, vis-à-vis global competitors?

Research Design and Methods

The task force research design was divided into three research modules, each three months in length, focused on understanding the applications of emerging technologies to the core elements of the intelligence process: collection, analysis, and distribution. The research methods were consistent across each module.

Literature Review: The CSIS study team conducted a comprehensive literature review to baseline the emerging technologies that were the focus of the task force and their potential application to intelligence missions. The review relied on recent or concurrent work of various national security and technology-focused research institutes focus on global technology trends and defense and intelligence applications; strategy documents on innovation from the ODNI, DOD, and other U.S. agencies; and academic and business literature exploring AI's application to analytic tasks and workflows.

Research Interviews: Throughout the research year, the task force conducted dozens of interviews and "deep-dive" briefings with a wide range of stakeholders. This included: science and technology experts from technology and defense industry firms and the research sector; intelligence, defense, and policy officials and science and technology experts from inside the U.S. government; and congressional staff. These interviews and deep-dives assisted the CSIS study team in deepening knowledge on key science and technology aspects of emerging technologies, their potential intelligence applications, and the barriers, challenges, and limitations of technology adoption in intelligence missions.

Task Force Meetings: CSIS convened three formal meetings of the task force during the project year, coinciding with each research module. The meetings included the task force commissioners, CSIS research team, outside technology experts, and select leaders and experts from the U.S. government. The purpose of these meetings was to preview the initial findings of each research phase, solicit feedback and additional perspectives from participants, and begin identifying initial key findings and recommendations for the final report.

APPENDIX B: GLOSSARY OF TERMS

Artificial Intelligence (AI): "The ability of a computer system to solve problems and perform tasks that would otherwise require human intelligence," for example, recognizing patterns, learning from experience, drawing conclusions, and making predictions[92]; "systems that extend human capability by sensing, comprehending, acting, and learning."[93]

Cloud Computing: "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)."[94]

Computer Vision: "A field of study that aims to analyze, extract, and understand objects and relationships from within single or multiple images."[95]

Deep Learning: "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."[96]

DevSecOps: "An organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor."[97]

Generative Adversarial Networks (GANs): "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."[98]

Graphics Processing Unit (GPU): "Specialized electronics designed to perform rapid mathematical functions to render images, animations, and videos."[99]

Machine Learning (ML): "The field of study interested in building computational systems that can improve their own performance of some task."[100]

Natural Language Processing (NLP): "A field of study that aims to analyze and understand human language communications both spoken and textual. Can include analysis and generation of language."[101]

Synthetic Biology: "A field of science that involves redesigning organisms for useful purposes by engineering them to have new abilities. . . . Redesigning organisms so that they produce a substance, such as a medicine or fuel, or gain a new ability, such as sensing something in the environment, are common goals of synthetic biology projects."[102]

APPENDIX C: SUMMARY OF TASK FORCE RECOMMENDATIONS

Applications

COLLECTION

1. Acting as the IC's HUMINT mission manager, the director of CIA, in consultation with other IC leaders, should pilot multiple initiatives designed to test the current and likely future impacts of emerging technologies on human intelligence operations.

2. The director of CIA and the director of NSA should co-lead an IC **advanced tech-enabled hard target strategic planning initiative**.

3. IC leadership should empower, staff, and resource DNI representatives in the foreign field to assemble **forward collection teams** to push AI-enabled collection and analysis closer to operators in contested areas.

4. IC collection agencies—particularly the CIA and NSA—in coordination with Congress should aim to **double the billets provided to S&T targeting and collection** of emerging and disruptive technologies by 2023.

5. The ODNI should facilitate a focused discussion with the White House to raise the priority assigned to **S&T in the National Intelligence Priorities Framework (NIPF)** and in agency internal collection requirements.

6. The ODNI, through the National Counterintelligence and Security Center, should review the current capabilities of the IC's China-focused CI cadre and what skill sets will be needed, including Chinese language capabilities and understanding of emerging tech, to counter the next generation of CI threats.

7. The ODNI, in partnership with the National Academy of Sciences, should sponsor a **study on the potential intelligence collection applications and implications of synthetic biology** and associated technologies.

8. IC collection agencies should **invest in AI-embedded sensors** to pre-process and sort collected data "at the edge" or at the point of collection, reducing the latency and amount of information transmitted to users.

ANALYSIS

9. IC analytic agencies should move rapidly to **procure, adapt, and integrate commercial off-the-shelf AI applications** using machine learning and natural language processing for traffic optimization, summarization, and categorization.

10. The CIA Directorate of Analysis should form an **AI-OSINT Red Cell**, equipped with cutting-edge AI tools, access to data and data scientists,

and training to test and demonstrate the utility and application of AI/ML technologies in open-source analysis and speed up technology risk mitigations where needed.

11. IC analytic directorates and mission centers should move swiftly to **increase analysts' ability to access OSINT and PAI reporting** on unclassified systems that are integrated into their classified workspace.

12. IC agencies with regionally focused analytic mission centers should establish **foreign S&T as a core analytic discipline** and integrate S&T analysts into country analytic units.

13. Assuming the continued successful operation of the IC Predictions Market, the National Intelligence Council should create a **new product line** that includes quarterly updates on key strategic questions posted to the IC Predictions Market. Most key judgments in NIC products should also include a forecast from the ICPM.

14. IC analytic components should sponsor **forecasting tournaments** that compare human judgments, AI models, and combinations of the two to forecast real-world events.

15. The CIA's Sherman Kent School for Intelligence Analysis should add to its curriculum for analysts **a module on educating policymakers on the use of AI in intelligence** as part of preparation for interacting with senior policymakers.

DISTRIBUTION

16. The ODNI, in conjunction with intelligence production staffs such as the PDB, should initiate a study on what changes to data architecture, engagement metrics, and customer modeling will be required to **apply AI and data analytics to customer feedback** while maintaining customer confidentiality. The findings should be briefed to senior policymakers at the National Security Council, Departments of Defense and State, other PDB recipients, and Congress.

17. The IC should develop an emerging technology training course, or **AI boot camp, for senior leaders** and intelligence customers.

18. Policymakers should also take a more **active role in telling the IC what products and delivery tools are most useful**. The NSC should more routinely issue guidance that establishes intelligence production priorities, what technologies should be enhanced, promulgated, scrapped, or developed, and a clear demand signal for incorporating AI and OSINT into finished intelligence products.

19. The IC should **establish an intelligence experience "skunkworks,"** bringing IC production staffs, briefers, and analysts together with data science, data visualization, VR/AR, UI/UX, and mobile device engineers and experts to create, test, and evaluate innovative products and services.

20. IC production teams, such as the PDB or CIA WIRe, should **develop an "Analyst Live" broadcast** channel for senior analysts and authors of new products to provide real-time video analysis of current events.

21. IC agency leaders should incentivize mission centers to encourage and reward analysts for **cultivating relationships with mid-level policy customers** and working with production staffs to exploit emerging technologies for digital delivery and engagement. IC organizations routinely serving policymakers at the secret and unclassified level, such as State Department INR, should be the leading edge of experimentation and implementation.

22. IC analytic agencies should leverage emerging technologies to **deepen partnerships with key non-PDB customers**, focusing on common and serious intelligence needs, such as a common operating picture in key theaters, intelligence sharing with host-nation and coalition partners, and sorting out what is "real" and "not real" for influence operations.

23. The ODNI should investigate the benefits and risks of using **AI/ML for instantaneous decisions about distribution**, determining "need to know" based on user attributes (location, echelon, time horizon) instead of traditional classification accesses and labeling, and develop a pilot program to test a new distribution model.

24. The ODNI, with assistance from In-Q-Tel and IARPA, should explore investments in **distributive ledger and blockchain** technology for enabling rapid intelligence sharing outside IC networks in zero or near-zero trust environments, such as the U.S. private sector and foreign liaison.

OSINT

25. The ODNI, in conjunction with Congress, should commission a specific study on how the IC's OSINT mission should be organized.

26. The ODNI should designate an OSINT lead to spearhead a IC-wide, cross-functional effort focused on driving and improving the integration of OSINT into IC tradecraft, workflows and analytic products.

27. The IC should establish unclassified OSC forward offices near key technology and talent hubs, starting with the San Francisco Bay Area.

Enablers

WORKFORCE AND ORGANIZATIONAL CULTURE

28. The IC should articulate **a new IC talent acquisition and management strategy** that determines the core attributes of a premier IC workforce for the future and how the IC can attract and retain that force.

29. The CIA Directorate of Operations (DO) and other **HUMINT organizations should prioritize hiring of candidates with existing**

STEM capabilities, alongside enduring priorities such as foreign language and cultural expertise.

30. **All-source analysis organizations should emphasize recruiting candidates with STEM backgrounds**, particularly those who also have education and skills in key regions and functional areas.

31. The IC should **increase the number of IC positions requiring only secret clearance**, particularly in technical fields, and unclassified positions focused on open source, to help acquire talent who are unable or do not want to receive a TS/SCI clearance.

32. The IC should continue **virtual internships and externships**, including during the academic year.

33. The IC should **establish "STEM pay,"** similar to foreign language pay, and hiring bonuses for any IC employee employing STEM skills in their day-to-day mission.

34. The IC should explore with Congress and the DOD the potential for **graduates of the recently proposed U.S. Digital Service Academy and STEM Corps to join positions in the IC**, including agencies outside DOD agencies, such as the ODNI and CIA.

35. The IC should, even while training operators and analysts, also **prioritize digital literacy for contracting and procurement officers, budget analysts, and security personnel** who are often the ultimate deciders of technology acquisition. This training should include best practices in DevSecOps, modules on how AI and other tools are to be applied to missions and understanding how these officers fit into technology transformation.

36. The U.S. HUMINT community should urgently **develop and field-test new doctrine and train the next generation of officers in the tradecraft** required to securely collect intelligence from human sources in a fully digitized world. Field tradecraft courses should include training on AI and associated technologies and integration into operations, including simulations and exercises.

37. The curriculum of the CIA's Sherman Kent School for Intelligence Analysis should be adapted to **develop baseline digital literacy** for all analysts and expanded training in data science and AI/ML applications for analysts seeking to regularly apply these tools.

38. The IC's **STEM cadre should receive more extensive education and training on core collection, analysis, and covert action missions** and how STEM skills and capabilities can be integrated.

39. The CIA, DIA, and other all-source analysis organizations should **establish an Analytic Team of the Future** initiative, envisioning how to integrate technologists into analytic units to hone and tailor AI applications for analysis and evolve analytic tradecraft.

40. The CIA should continue to build out t**he recently established CIA Labs** for many reasons, including for its creative approach to allowing open agency officers to take credit for their innovation and IP through patents and global recognition.

41. IC HUMINT organizations should **establish an S&T case officer cadre**, with specialized training and mission assignments focused on collecting intelligence on foreign S&T plans, intentions, and capabilities. S&T case officers should have a similar path to senior HUMINT leadership positions as any other cadre.

42. All-source analytic organizations should similarly **establish AI analyst cadres**, focused on assessing foreign AI systems and S&T capabilities and their integration into statecraft, economic competitiveness, and military and intelligence operations.

43. IC organizations, particularly the CIA, should **expand the opportunities available for S&T targeters, data scientists, and researchers to serve in overseas assignments** as well as in locations across the United States.

ACQUISITION AND ADOPTION

44. The next **DNI should establish an Intelligence Innovation Initiative**.

45. The DNI should definitively designate the principal deputy DNI (PDDNI) as the IC's senior official responsible for innovation across the IC, and the innovation portfolio as the PDDNI's top priority.

46. The DNI and PDDNI should review the roles, missions, staffing, and organization of the ODNI to ensure it is optimized to drive a coherent, strategy-driven approach to catalyzing innovation across the IC.

47. The PDDNI, working with agency leaders, should **develop an innovation risk framework** that aids organizations in weighing both the risk of failure/loss and the opportunity cost of inaction when considering acquisitions and adoptions of innovative new capabilities.

48. The PDDNI should lead a comprehensive review to r**efresh acquisition and requirements policies**, to include software-specific policies and practices, rapid contracting, and flexible authorities, and to incentivize risk-taking and exercising authorities where they already exist.

49. The IC should further develop a **new software acquisition model** to guide agency procurement and pilot a "software as a service" model inside a mission agency. The IC should adopt many of the best practices outlined in the Defense Innovation Board's Software Acquisition and Practices (SWAP) Study.

50. The IC should continue to develop flexible acquisition mechanisms, including an **IC Acquisition Consortium** that is authorized to issue umbrella contract authorities to provide an IC-wide contract vehicle(s) for agencies to leverage.

51. The IC should prioritize **training of contracting officials on rapid authorities** and new approaches for procurement of software, AI, and associated advanced technologies.

52. The DNI and the secretary of defense should establish a **Tri-Chair Steering Committee on Emerging Technology** across the DOD and IC, consisting of the PDDNI, deputy secretary of defense, and vice chairman of the joint chiefs of staff, as was also recommended by the National Security Commission on AI.

53. The IC should catalyze DOD-IC collaboration forums for greater collaboration and sharing of best practices and lessons learned, to include an annual DOD-IC AI Summit and **annual DOD-IC Acquisition Conference**.

54. The ODNI should examine options for creating an ICWERX, housed under ODNI CTO, as a premier innovation and procurement hub with sufficient resources and personnel. Alternatively, or in addition, the IC could establish cells in other hubs such as AFWERX and SOFWERX to combine investment resources with DOD elements where priorities align.

55. IC leadership, perhaps under the auspices of the Intelligence Innovation Board and In-Q-Tel, should facilitate more regular and direct **conversations between mission directorates and technology providers**.

56. IC leadership should, in rebalancing risk tolerance, encourage agencies and directorates to pursue a rapid prototyping approach, more quickly pushing out **prototypes and beta versions of software and other technologies** for user feedback and continuous iteration, instead of waiting for the 100 percent solution before deployment.

57. IC elements should encourage integrating **technology providers and procurement officers into user experimentation, wargaming, modeling, and simulations** to help develop intelligence-operational concepts with emerging technology experts.

STRATEGIC PARTNERSHIPS (COMMERCIAL, RESEARCH, FOREIGN)

Commercial

58. The IC should establish a **U.S. Intelligence Innovation Board (IIB)**.

59. The ODNI CTO and In-Q-Tel should create a unified **IC venture engagement strategy** for interacting with the U.S. venture capital community to access, adapt, and deploy innovative technology, led by In-Q-Tel.

60. In-Q-Tel and the ODNI should host a **biannual UI/UX Forum** that brings together software and application designers from firms supporting the IC with IC technology end users to test and solicit feedback on UI/UX for intel applications and products being developed.

61. The IIB, In-Q-Tel, and the OSC should convene an **annual Worldwide Technology Threat Assessment conference** for the IC and private sector firms focused on assessing emerging and disruptive technologies. The IC—under the NIC or OSC auspices—could additionally craft an unclassified assessment of the key findings. Congress could hold a Technology Threat Assessment hearing to align legislators and garner greater attention to these issues.

62. Through the IIB, the IC should explore the potential for **more robust data and algorithm development and sharing** with select, vetted private sector partners, particularly in the financial sector, commercial imagery and other space-based collection firms, and data analytics firms.

63. The ODNI should **establish an Intelligence Innovation Fellowship** that selects 8 to 10 IC professionals to spend a year on rotation fully away from the IC embedded with a technology organization, with the IIB and In-Q-Tel helping facilitate placement. Additionally, IC organizations should at a minimum loosen restrictions and, ideally, actively encourage officers to take leave without pay to pursue paid opportunities in the technology sector while maintaining their eligibility and clearance status to return to the IC.

64. The ODNI should also **establish an Innovator in Residence** program, selecting 8-10 private sector technologists and entrepreneurs with interest or experience providing technology to the IC to embed in IC organizations. Depending on clearance levels, innovators could be placed in IC research organizations such as IARPA or CIA Labs or embedded in mission directorates and centers.

65. The IC should **establish a biotechnology public-private partnership** with U.S. commercial biotechnology firms and other biotech research organizations willing and able to share data, insights, and analysis of emerging biotechnologies and applications with implications for U.S. national security.

Research

66. IC R&D entities such as CIA Labs and IARPA should **expand efforts with U.S. universities to collaborate and sponsor research, development, testing, and engineering of S&T solutions** for intelligence problems, particularly in the AI space.

67. The IC should **establish robust academic outreach offices** that include intelligence officers in residence and university fellowships, guest speaker series, and online lectures on intelligence topics to be used on campus.

68. The IC should **increase the number of IC summer internship programs for college STEM majors** after their freshman year. This is a major window of opportunity, since few major tech companies hire engineering students that early.

69. The IC should **build upon the DOD's Hacking for Defense program**, with IC-centric versions focused on real-world, policy-relevant intelligence problems.

70. The IC should **create a high-profile IC fellowship program for 25 to 50 graduating STEM students from top universities**.

71. IC agencies should **create formal AI partnerships with the research sector** that could include:

    - Verifying and validating algorithms, performing testing and evaluation (T&E) on IC models, and collaborating on new AI application methodologies;
    - Coordinating to identify data sets for researchers to train on and creating rubrics for scoring and testing; and
    - Creating joint competitions such as an unclassified AI Olympics to generate ideas for solving real IC problems with analogous data sets and interest from early-stage researchers in priority areas, particularly if grant or prize funding is attached.

Foreign Partners

72. The ODNI should lead interagency efforts to **build a FVEY Cloud** as the basis for technological collaboration and intelligence generation with its closest intelligence allies. A FVEY cloud would serve not only as the primary platform for data and intelligence sharing but also as a shared common foundation for algorithm and application development and joint deployment of AI to enable missions and workflows worldwide.

73. IC agencies should **support AI Talent Exchanges**, sponsoring S&T analysts, data scientists, engineers, and researchers to spend one to two years embedded in foreign partner organizations working on joint intelligence innovation. The IC could start with pilots with FVEY allies and look to expand to other like-minded partners.

74. The ODNI should **invite FVEY agency and commercial sector participation in the Intelligence Innovation Board** to build common understanding of emerging technology trends and foster joint strategic partnerships with industry.

75. IC collection agencies should **develop and implement a Joint Tradecraft Initiative** with select allies and partners—multilatrally or bilaterally—to envision and develop new collection tradecraft harnessing emerging technologies. DNI representatives in the foreign field should be given the training, resources, and authorities to oversee and execute the initiative in the field, with support from headquarters agencies.

76. The U.S. IC, working with its commonwealth allies, should **harness a FVEY Cloud for an Allied Algorithm Project**, building common data

lakes to collaborate on training, testing, validating, and employing algorithms for common intelligence mission application.

77. The ODNI CTO should **sponsor an Automated Tearline Project** that uses AI to develop rapid, automated intelligence sanitization and dissemination applications for use with allies and partners.

78. The OSC should take the lead in **developing a weekly OSINT analytic product generated jointly with FVEY allies**, exploiting AI and data analytics for timely analysis on a particular global issue or trend conducive to these tools, such as foreign S&T development or regional instability indicators and warning.

STRATEGIC R&D AND NEXT GENERATION TECHNOLOGIES

79. The DNI should consider further empowering the ODNI Office of Science and Technology and elevating its director to serve as the U.S. IC chief technology officer (CTO).

80. The IC, with congressional support, should **create a Technology Investment Fund administered by the ODNI** and focused on developing new IC-specific capabilities and providing multiyear flexibility to meet agile acquirements.

81. In addition to regular intelligence support to IARPA, DARPA, and other U.S. government advanced research agencies, the ODNI should leverage its new IC Net Assessment Office to **conduct an annual Technology Net Assessment** of U.S. and key adversary technology strategies, future capabilities, and potential countermoves to U.S. investments.

82. ODNI S&T and IARPA should **conduct annual roadshows** to IC operational and analytic directorates and mission centers to educate and demonstrate to users the latest emerging tech with potential mission applications.

83. Going the other direction, directorates and missions should sponsor and incentivize collectors and analysts, particularly those with foreign S&T specializations, for **rotational opportunities at IARPA** to gain firsthand experience with innovation.

84. The IC and Congress should work together to **set aside secure and significant funding for basic research and fundamental scientific exploration**. Congress must protect those budgets from being harvested for operational and maintenance budget shortfalls while ensuring the research is in line with broad intelligence and national security priorities

85. IC research and S&T organizations should **set aside a certain percentage of total billets—perhaps starting at 10 percent and gradually increasing—that only require secret clearances** and collaborate with commercial and research sector partners to identify project roles that require no clearance at all.

86. ODNI—using the IIB and partnerships with academic and national labs—should **explore the creation of the Tech-Intel Reserve Corps**. Like military reserve units, these tech experts could conduct annual exercises and provide monthly research support to IC agencies on secret or open-source research projects while receiving IC training and compensation.

INFRASTRUCTURE, ARCHITECTURE, AND SECURITY AND ASSURANCE

87. In conjunction with IC agencies, the **ODNI should conduct a comprehensive Covid-19 remote work review** of what has been achieved through the pandemic, including an assessment of risks and benefits, lessons learned, and recommendations for the future of IC remote work.

88. IC infrastructure and technology leaders should collaborate with operational agencies and directorates to prioritize **building a forward-deployed cloud**, focused on delivering secure, resilient, rapidly deployed cloud services and AI applications to operators at the edge.

89. The IC should **build on the IC Information Technology Enterprise (ITE) and C2S toward an interagency IC Cloud**.

90. The recently established IC chief data officer should work with the IC CIO to **develop common data conditioning, tagging, and labeling standards**, including for metadata, that will facilitate cross-IC usage and application.

91. The IC **should invest in synthetic data** (and associated storage and compute power) both to expand the number and size of training data sets and reduce the time and burden of human analysts doing labeling.

92. The IC chief data officer should spearhead an interagency initiative to **assemble large-scale classified training data sets** available to any IC agency, with data conditioned according to the standards framework described above.

93. The PDDNI should also push for individual agency CIOs and data managers to identify ways to **reduce barriers to entry and promote data-sharing and AI interoperability through open architecture and more flexible access authorities**.

94. The ODNI, with agency CIOs and S&T directorates, should l**aunch a Cross-Domain Challenge** to test the feasibility of building and training IC-specific algorithms and models on multi-INT data and both classified and open sources.

95. IC agencies should prioritize **investment in emerging security technologies**, to include AI-enabled cyber defense, advanced cryptography, countering adversarial AI, threat intelligence/anomaly detection, and supply chain security.

96. IC agencies should **adopt best practices in DevSecOps** for software development and deployment, including from the private sector and innovators in the DOD, such as the JAIC.

97. The ODNI in partnership with the DOD should **establish a National AI/ML Red-Teaming Center** with focus on simulating and testing AI systems against adversarial AI.

98. In addition to red-teaming, the ODNI and IC agencies **should adopt TEVV (test and evaluation, verification and validation) best practices and standards**, leveraging its strategic partnerships with the private sector, research community, and foreign allies for lessons learned.

99. IC agencies should **explore historic assurance** models, including the NSA's Information Assurance mission and the NGA's recently built Office of GEOINT Assurance, to identify best practices.

ETHICS AND GOVERNANCE

100. The ODNI Office of Civil Liberties, Privacy, and Transparency, in conjunction with relevant National Intelligence Managers, S&T directorates, and CIOs, should **launch an Open Source and Civil Liberties Initiative**.

101. IC agencies should collaborate to **determine common standards and best practices for AI explainability in AI-enabled workflows and analytic products**, to include how certain types of algorithms should or should not be applied and how to clearly explain AI application and implications in intelligence products. IC explainability practices should conform not only to analytic tradecraft and review standards but also to IC responsibilities for transparency and accountability in its work for policymakers, Congress, and the public.

102. IC agencies should also leverage strategic partnerships with the private and research sectors for **ideas and best practices on transparency and explainability in AI-enabled workflows**, such as use of model cards for AI and ML models.

103. The ODNI Office of Mission Integration should gather an IC working group to **develop best practices for understanding, documenting, mitigating, and communicating AI bias in AI-enabled workflows and products**.

ENDNOTES

Acknowledgments

1 House Permanent Select Committee on Intelligence, *Rightly Scaled, Carefully Open, Infinitely Agile: Reconfiguring to Win the Innovation Race in the Intelligence Community* (Washington, DC: 2020), https://intelligence.house.gov/uploadedfiles/final_start_report_v4.pdf.

Scenesetter

2 National Security Commission on Artificial Intelligence, *Interim Report* (Washington, DC: 2019), https://drive.google.com/file/d/153OrxnuGEjsUvlxWsFYauslwNeCEkvUb/view; and Department of Defense AI Strategy, 2018.

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

4 Elsa Kania, "Chinese Military Innovation in Artificial Intelligence," Testimony before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion, June 7, 2019, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence.pdf; and Samuel Bendett, "Russia's AI Quest in State-Driven—Even More than China's. Can It Work?," Defense One, November 25, 2019, https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519/.

5 Cloud computing is 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*. Office of the Director or National Intelligence (ODNI), *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines* (Washington, DC: January 2019), https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf; Greg Allen and Taniel Chan, *Artificial Intelligence and National Security* (Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs, July 2017), https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf; and Kelley M. Sayler, *Artificial Intelligence and National Security*, CRS Report No. R45178 (Washington, DC: Congressional Research Service, November 2019), https://fas.org/sgp/crs/natsec/R45178.pdf.

6 Computer vision is "a field of study that aims to analyze, extract, and understand objects and relationships from within single or multiple images." Natural language processing is 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*.

Strategic Threats and Challenges

7 Kania, "Chinese Military Innovation in Artificial Intelligence."

8 Kai-Fu Lee, *AI Superpowers: China Silicon Valley, and the New World Order* (Boston: Houghton Mifflin Harcourt, 2018), 83.

9 Samuel Bendett, "Russia's AI Quest in State-Driven – Even More Than China's. Can It Work?," Defense One, November 25, 2019, https://www.defenseone.com/ideas/2019/11/russias-ai-quest-state-driven-even-more-chinas-can-it-work/161519/; and National Security Commission on Artificial Intelligence, *Interim Report*.

10 Kania, "Chinese Military Innovation in Artificial Intelligence."

11 Jenna McLaughlin and Zach Dorfman, "'Shattered': Inside the secret battle to save America's undercover spies in the digital age," Yahoo News, December 30, 2019,

https://news.yahoo.com/shattered-inside-the-secret-battle-to-save-americas-undercover-spies-in-the-digital-age-100029026.html; and Steven Feldstein, "The Global Expansion of AI Surveillance," Carnegie Endowment for International Peace, September 17, 2019, https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847.

12 Elsa Kania, Dahlia Peterson, Lorand Laskai, and Graham Webster, "Translation: Key Chinese Think Tank's 'AI Security White Paper' (Excerpts)," New America Foundation, February 21, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-key-chinese-think-tanks-ai-security-white-paper-excerpts/; and "Chinese satellite uses quantum cryptography for secure videoconference between continents," *MIT Technology Review*, January 30, 2018, https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/.

13 National Security Commission on Artificial Intelligence, *Interim Report*.

14 ODNI, *The AIM Initiative*.

15 Will Douglas Heaven, "OpenAI's new language generator GPT-3 is shockingly good—and completely mindless," *MIT Technology Review*, July 20, 2020, https://www.technologyreview.com/2020/07/20/1005454/openai-machine-learning-language-generator-gpt-3-nlp/.

16 In generative adversarial networks, 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*.

17 Sean Gourley, "To fight disinformation, we need to weaponize the truth," *Wired*, January 6, 2020, https://www.wired.co.uk/article/fix-disinformation-facts.

Applications

18 Brian Katz, "The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection," CSIS, *CSIS Briefs*, July 13, 2020, https://www.csis.org/analysis/collection-edge-harnessing-emerging-technologies-intelligence-collection.

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

20 Expert remarks from CSIS Technology and Intelligence Task Force meeting, April 2020.

21 Ibid.

22 Ibid.; and ODNI, *The AIM Initiative*.

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

24 Ibid.

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

26 Ibid.

27 Kania, Peterson, Laskai, and Webster, "Translation: Key Chinese Think Tank's 'AI Security White Paper' (Excerpts)"; and "Chinese satellite uses quantum cryptography for secure videoconference between continents," *MIT Technology Review*.

28 National Security Commission on Artificial Intelligence, *Interim Report*.

29 House Permanent Select Committee on Intelligence, *The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China* (Washington, DC: September 2020), https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf.

30 50 USC Section 3093, "Presidential approval and reporting of covert actions," https://www.govinfo.gov/content/pkg/USCODE-2014-title50/pdf/USCODE-2014-title50-chap44-subchapIII-sec3093.pdf.

31 Katz, "The Analytic Edge."

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

33 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/.

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

35 Raymond, "How Emerging AI Technologies Can Help Us Think 'Smarter'."

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

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

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

39 Raymond, "How Emerging AI Technologies Can Help US Think 'Smarter'."

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

41 ODNI, *Strategic Plan to Advance Cloud Computing in the Intelligence Community* (Washington, DC: June 2019), https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf.

42 National Security Commission on Artificial Intelligence, *Interim Report*.

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

44 Ibid.

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

46 Ibid.

47 ODNI, *The AIM Initiative*.

48 Remarks by senior IC official to the CSIS Technology and Intelligence Task Force, October 2020.

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

50 Ibid.

51 Remarks by senior IC official to the CSIS Technology and Intelligence Task Force, October 2020.

52 Ibid.

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

54 Ibid.

55 Remarks by former senior ODNI official to the CSIS Technology and Intelligence Task Force, October 2020.

56 Ibid.

57 U.S. defense software firm research interview by CSIS Intelligence and Technology Task Force, September 2020.

58 Katrina Mulligan, Matt Olsen, and Alexandra Schmitt, "What the Intelligence Community Doesn't Know Is Hurting the United States," Center for American Progress, September 18, 2020, https://www.americanprogress.org/issues/security/reports/2020/09/18/490532/intelligence-community-doesnt-know-hurting-united-states/.

59 Brian Katz, "Policy and You: A Guide for Intelligence Analysts," War on the Rocks, February 5, 2019, https://warontherocks.com/2019/02/policy-and-you-a-guide-for-intelligence-analysts/.

60 Brian Katz, "Intelligence and You: A Guide for Policymakers," War on the Rocks, November 14, 2018, https://warontherocks.com/2018/11/intelligence-and-you-a-guide-for-policymakers/.

Enablers

61 Expert remarks at CSIS Technology and Intelligence Task Force meeting.

62 Ibid.

63 U.S. intelligence organization research interview by CSIS Intelligence and Technology Task Force, May 2020.

64 U.S. intelligence organization research interview; and U.S. defense and technology firm research interview, March 2020.

65 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/.

66 "Second Quarter Recommendations," National Security Commission on Artificial Intelligence, *Quarterly Series*, No. 2, July 2020, https://drive.google.com/file/d/1hgiA38FcyFcVQOJhsycz0Ami4Q6VLVEU/view; and U.S. Congress, House, *STEM Corps Act of 2020*, H.R. 6526, 116th Cong., 2nd sess., April 17, 2020, https://www.congress.gov/bill/116th-congress/house-bill/6526/text.

67 DevSecOps is an organizational software engineering culture and practice that aims at unifying software development (Dev), security (Sec) and operations (Ops). The main characteristic of DevSecOps is to automate, monitor, and apply security at all phases of the software lifecycle: plan, develop, build, test, release, deliver, deploy, operate, and monitor. Department of Defense Chief Information Officer, *DoD Enterprise DevSecOps Reference Design* (Washington, DC: DOD, August 2019), https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference%20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583.

68 Defense Innovation Board, *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, DC: U.S. Department of Defense, May 3, 2019), https://media.defense.gov/2019/Apr/30/2002124828/-1/-1/0/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINAL.SWAP.REPORT.PDF.

69 "Summary of the National Security Commission on Artificial Intelligence's First Quarter Recommendations," National Security Commission on AI, March 2020, https://drive.google.com/file/d/1RBwXf0SCaKPczcyfwfu1CA1ZDci4oxBx/view.

70 ODNI, *The AIM Initiative*.

71 U.S. synthetic biology firm research interview by CSIS Intelligence and Technology Task Force, May 2020.

72 U.S. intelligence research organization research interview by CSIS Intelligence and Technology Task Force, September 2020.

73 ODNI, *Strategic Plan to Advance Cloud Computing in the Intelligence Community* (Washington, DC: June 2019), https://www.dni.gov/files/documents/CIO/Cloud_Computing_Strategy.pdf.

74 Ibid.

75 ODNI, *The AIM Initiative*.

76 Remarks by senior IC official to the CSIS Technology and Intelligence Task Force, July 2020.

77 U.S. technology and cloud-provider firm research interview by CSIS Intelligence and Technology Task Force, June 2020; ODNI, *The AIM Initiative*; and Cruickshank, "The ABCs of AI-Enabled Intelligence Analysis."

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

79 National Security Commission on Artificial Intelligence, *Interim Report*; and ODNI, T*he AIM Initiative*.

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

81 Ibid.

82 Michele Flournoy, Avril Haines, and Gabrielle Chefitz, "Building Trust through Testing: Adapting DOD's Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems," WestExec Advisors, October 2020, https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf.

83 Ibid.

84 "Artificial Intelligence Ethics Framework for the Intelligence Community," ODNI, June 2020, https://www.dni.gov/files/ODNI/documents/AI_Ethics_Framework_for_the_Intelligence_Community_10.pdf.

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

86 Ibid.

87 Sayler, *Artificial Intelligence and National Security*; and 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/.

88 ODNI, "Artificial Intelligence Ethics Framework for the Intelligence Community."

89 "Model Cards," Google, https://modelcards.withgoogle.com/about.

90 Gartin, "Thinking About the IC's Talent Management Issues in an AI/ML Environment."

91 ODNI, "Artificial Intelligence Ethics Framework for the Intelligence Community."

Appendix B: Glossary of Terms

92 National Security Commission on Artificial Intelligence, *Interim Report*.

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

94 ODNI, *Strategic Plan to Advance Cloud Computing in the Intelligence Community*.

95 ODNI, *The AIM Initiative*.

96 National Security Commission on Artificial Intelligence, *Interim Report*.

97 Department of Defense Chief Information Officer, *DoD Enterprise DevSecOps Reference Design*.

98 National Security Commission on Artificial Intelligence, *Interim Report*.

99 ODNI, *The AIM Initiative*.

100 Ibid.

101 ODNI, *The AIM Initiative*.

102 "Synthetic Biology," National Human Genome Research Institute, https://www.genome.gov/about-genomics/policy-issues/Synthetic-Biology.

COVER PHOTO ADOBE STOCK

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | **www.csis.org**