Stanford University
Human-Centered
Artificial Intelligence

MARCH 2021

The Moment of Reckoning: AI and the Future of U.S. Intelligence

Amy Zegart

THE U.S. INTELLIGENCE COMMUNITY FACES A MOMENT OF RECKONING and AI lies at the heart of it. Since 9/11, America's intelligence agencies have become hardwired to fight terrorism. Today's threat landscape, however, is changing dramatically, with a resurgence of great power competition and the rise of cyber threats enabling states and non-state actors to spy, steal, disrupt, destroy, and deceive across vast distances — all without firing a shot.

At the same time, new technologies are eroding the "decision advantage" that the U.S. has traditionally enjoyed. Until recently, intelligence was a superpower contest. Not anymore. The rapid global expansion of cell phones, internet connectivity, and commercial satellites has created a world awash in open-source data that can be collected, analyzed, and used by anyone. Today, geopolitical success, whether it's preventing war or advancing American economic interests, requires harnessing all this information to understand trends, events, threats, and opportunities faster and better than adversaries who are unencumbered by America's constitutional and ethical obligations to protect civil liberties and privacy. AI promises to be at the forefront of these new capabilities — with the potential to transform the collection, analysis, and dissemination of intelligence vital to American national security.

As I argue in my writing for *Foreign Affairs* as well as in a forthcoming book, the nation's lack of a coordinated strategy allows other countries and groups to level the intelligence playing field at the expense of the United States. For the U.S. to avoid the risks and maximize the opportunities of this technological era, policymakers need to act swiftly to ensure the Intelligence Community adapts, integrating AI into all of its processes in ways that augment human capabilities and reflect American values.

KEY TAKEAWAYS

- The Intelligence Community (IC) faces a moment of reckoning. If the IC cannot adopt AI and other emerging technologies successfully, it risks failure.
- AI is critical to maintaining America's decision advantage — helping intelligence agencies harness the explosion of open-source data with increased precision, speed, and analytic power to detect hidden and emerging patterns.
- AI's promise lies in augmenting human intelligence collectors and analysts, not replacing them.
- The most important near-term steps are developing a comprehensive intelligence and technology strategy, establishing a new open-source intelligence agency, making it easier to recruit scientific and engineering talent, and bridging the divide between government, industry, and academia.

Success will require much more than simply using new algorithms. It will require a reimagining the Intelligence Community (IC) and a new comprehensive strategy transforming the IC's organization, culture, and workforce to maintain decision advantage in a new technological era. A blue-ribbon intelligence reform commission should be convened to identify ways to build on the country's distinctive advantages as an open society with democratic values and further leverage our global reach to reinforce the natural edge we hold in collecting intelligence. A new open-source intelligence agency should be created to elevate open-source intelligence as well as provide a test bed for collaboration with industry to prototype new AI intelligence capabilities. Talent, too, will be critical: The IC needs to make it much easier to attract a workforce with the technological know-how to understand other nations' technological capabilities and better utilize our own. And policymakers need to continue working in earnest to bridge the divide between government and the tech sector to reconcile competing commercial incentives, privacy concerns, and national security interests.

Introduction: The Double-Edged Sword of Technology

Advances in technology like artificial intelligence tend to be a double-edged sword for intelligence collection and analysis: They generate opportunities for gain while also exposing the nation to new risks. Exponential improvements in pattern recognition and the optimization of digital weapons that AI makes possible

Even without artificial intelligence, this profusion in connectivity has already shown the potential to turn normal citizens into intelligence collectors either knowingly or unknowingly.

mean that the United States as well as its competitors and adversaries are able to make better decisions, faster. With data and threats moving at the speed of networks, intelligence must rely on AI to help humans keep up.

Opportunities and Risks

AI can improve both the scale of information that can be processed and the quality of intelligence products that result. Already, AI's pattern recognition capabilities enable analysts to scour the globe using geospatial imagery and identify key objects on the ground at superhuman speeds. In 2021, for example, one Stanford study reported that a machine learning algorithm could count trucks transiting from China to North Korea on hundreds of satellite images 225 times faster than an experienced human imagery analyst — with the same accuracy. AI can also enable human intelligence officers to better visualize networks of who knows who and whether an individual could be a potential asset to

recruit. And by automating the mundane, AI can allow analysts to spend less time doing basic tasks and more time on the value-added jobs that require higher-level thinking that only humans can perform — like considering alternative hypotheses.

With the explosion of open-source information coming from ever more smart devices connected to the internet, over half of the world's population is now online. Cell phones, tablet computers, and even fitness devices like a Fitbit can capture a wide range of activities around the world. Even without artificial intelligence, this profusion in connectivity has already shown the potential to turn normal citizens into intelligence collectors either knowingly or unknowingly. Social media companies, search engines, and online retail platforms collect, expose, and sell a great deal of information about users, which in turn provides a potential treasure trove of open-source information. According to one estimate, in 2019, on average people around the world produced 500 million tweets, sent nearly 300 billion emails, and posted 350 million photos to Facebook *every day*. AI has the potential to dramatically reduce the "noise" of all this data, improving both how much data can be processed and the insights that come from it — to find more needles in exponentially larger haystacks.

To be sure, secrets that have traditionally been the focus of intelligence will remain vital for tasks such as gauging the intentions of adversaries like North Korea's Kim Jong-un or for determining that Russian President Vladimir Putin was behind efforts to interfere with the 2016 American presidential election. But artificial intelligence offers new capabilities to marry open-source information with these secrets to serve the intelligence mission: providing tailored information to policymakers that reduces uncertainty and gives them decision advantage.

The United States should establish a stand-alone, open-source intelligence agency, because existing agencies that were all built to collect and analyze secrets will never give open-source intelligence the attention or resources it needs to succeed.

Policy Discussion

Inside the U.S. Intelligence Community, work is already underway to meet the challenges outlined above. The CIA's directorate for digital innovation, the National Geospatial-Intelligence Agency's AI initiatives, and cloud-computing efforts at the National Security Agency all show promise, but these efforts by themselves are nowhere near enough to leverage the full potential of this breakthrough technology. Although there are new Pentagon units to harness technological innovation and bipartisan national commissions on cybersecurity and artificial intelligence, what's needed now is a wholesale reimagining of intelligence for a new technological era that fully recognizes the scale of transformation we are living through. We face a "hinge of history" moment, with

emerging technologies poised to transform societies, economies, and politics in dramatic and unforeseen ways.

If American interests and values are to ultimately prevail, then the U.S. Intelligence Community needs to undertake a wide-ranging strategic effort to identify how AI can expand our intelligence capabilities while safeguarding civil liberties and addressing Americans' privacy concerns. In addition to convening an IC-wide strategy for sustaining the nation's technological advantage, the United States should establish a stand-alone, open-source intelligence agency, because existing agencies that were all built to collect and analyze secrets will never give open-source intelligence the attention or resources it needs to succeed.

The IC also needs to focus on people. Part of that effort involves implementing a host of reforms to make it easier to attract a STEM workforce. Another key component is continuing to improve collaboration with the private sector and academic communities that are pioneering AI advances to more quickly adopt new technologies and also work with tech companies to manage the clash between commercial incentives, privacy, and national security interests. Today, tech companies are facing national security responsibilities they don't want and intelligence agencies are seeking technological capabilities they don't have. Better public-private collaboration is needed to address both challenges.

Finally, the Intelligence Community should reorient the way it thinks about public engagement, with communications geared not just toward decision makers with security clearances who work inside the government, but increasingly to those outside and even the general public.

The Intelligence Community should reorient the way it thinks about public engagement, with communications geared not just toward decision makers with security clearances who work inside the government, but increasingly to those outside and even the general public.

The original article, **"Spies, Lies, and Algorithms,"** can be found here: https://www.foreignaffairs.com/articles/2019-04-16/spies-lies-and-algorithms, and the original piece, **"Intelligence Isn't Just for Government Anymore,"** can be found here: https://www.foreignaffairs.com/articles/united-states/2020-11-02/intelligence-isnt-just-government-anymore.

For more on reform proposals, see CSIS Report from the Technology and Intelligence Task Force.

Stanford University's Institute on Human-Centered Artificial Intelligence (HAI), applies rigorous analysis and research to pressing policy questions on artificial intelligence. A pillar of HAI is to inform policymakers, industry leaders, and civil society by disseminating scholarship to a wide audience. HAI is a nonpartisan research institute, representing a range of voices. The views expressed in this policy brief reflect the views of the authors. For further information, please contact **HAI-Policy@stanford.edu.**

Amy Zegart, PhD is chair of the Steering Committee on International Affairs and Security at the Stanford Institute for Human-Centered Artificial Intelligence (HAI); senior fellow at Stanford's Center for International Security and Cooperation (CISAC) at the Freeman Spogli Institute for International Studies; senior fellow at Stanford's Hoover Institution; and professor of political science, by courtesy.

Stanford University
Human-Centered
Artificial Intelligence

Stanford HAI: Cordura Hall, 210 Panama Street, Stanford, CA 94305-4101

T 650.725.4537 **F** 650.123.4567 **E** HAI-Policy@stanford.edu **hai.stanford.edu**