CSET at Three

PROGRESS
REPORT 2022

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

CSET PRODUCES DATA-DRIVEN RESEARCH at the intersection of security and technology, providing nonpartisan analysis to the policy community. A policy research organization within Georgetown University's Walsh School of Foreign Service, CSET is currently focusing on the effects of progress in artificial intelligence (AI), advanced computing, and biotechnology. We seek to prepare a new generation of decision-makers to address the challenges and opportunities of emerging technologies.

BY THE NUMBERS

165 data-rich reports

data holdings include nearly
65 analysis-ready datasets

53 full-time staff

just under
240 million scholarly documents

357 original translations
of key documents from Russia and China
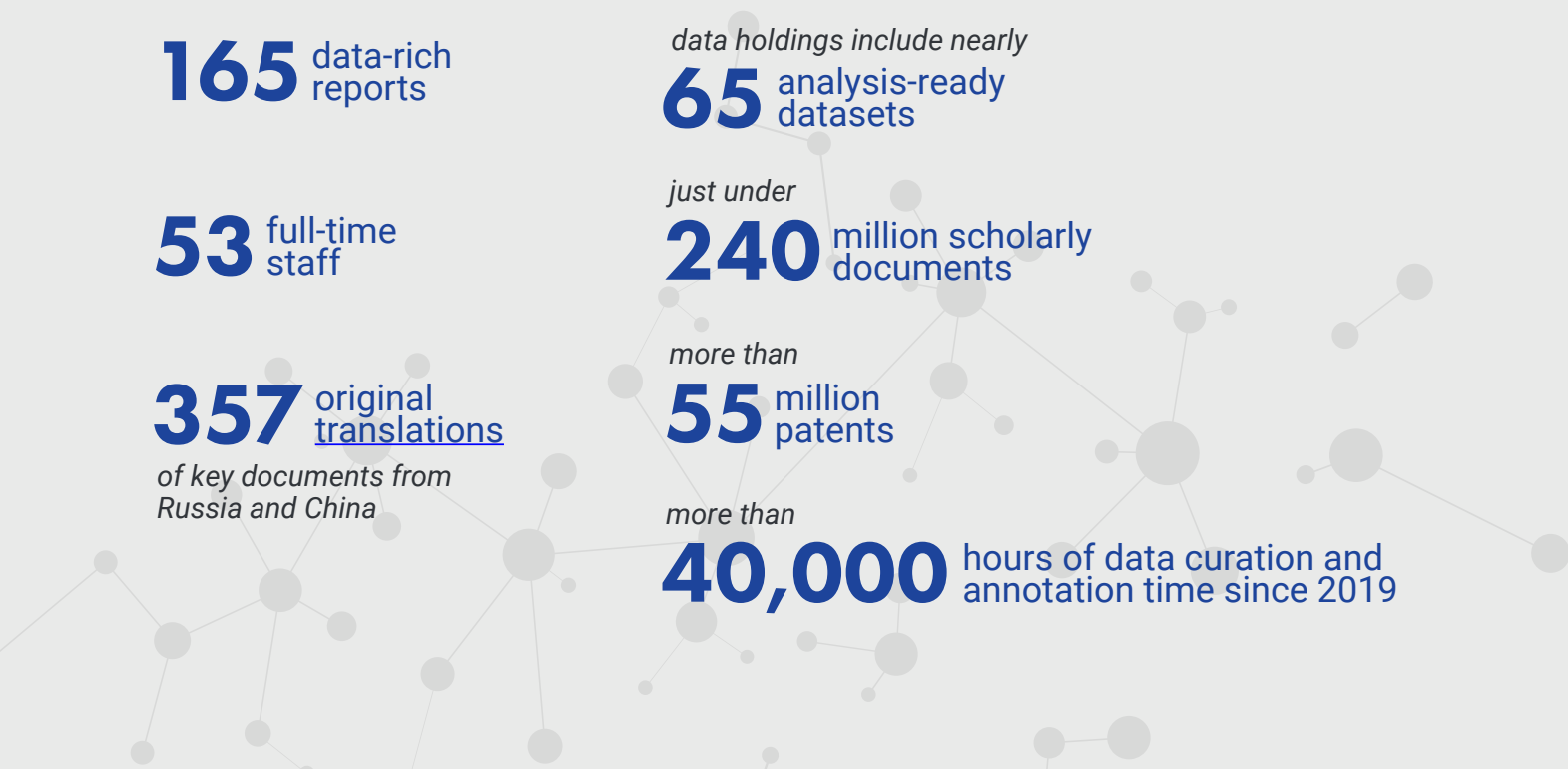
more than
55 million patents

more than
40,000 hours of data curation and annotation time since 2019

DIRECTOR'S LETTER

Watching CSET grow these last three years has been thrilling. In December 2018, we had two employees and high hopes that we could provide a new model for evidence-driven policy analysis that wrestled with the pivotal emerging technology and security questions of our time. We were prepared to spend the required resources to gather, fuse, and translate primary data sources at a large enough scale to meaningfully answer policy-relevant questions about artificial intelligence (AI), machine learning (ML), and advanced computing. We set out to assemble a first-rate team to achieve two main goals: produce quality, insightful work that influences policy outcomes, and prepare members of that team to go on to careers in policymaking themselves.

Since then, we have employed a total of 95 staff (and 78 students) who have collaboratively connected policymakers to impactful analysis of emerging technologies and their security implications. It is exciting that we have already had 19 former staff and students transition to public service roles. We've produced hundreds of actionable written products and translations that directly speak to pressing policy questions and open decisions, plus we've experimented with and released interactive public research resources to help CSET's stakeholders answer their own questions.

I'm excited to see CSET continue to provide unique, evidence-driven research that is easy for decision-makers to read and use. I look forward to continuing to help decision-makers successfully navigate critical issues, such as AI/ML-relevant failure modes in cybersecurity and beyond, tracking risky biotech research, and controlling sensitive enabling technology and monitoring supply chains in coordination with allies. I aspire for CSET's analysis to bolster the development of a strong emerging technology workforce, understand the international emerging technology landscape, and contribute insights to the innovation ecosystem. I am also excited to experiment with partnerships that provide foundational insights in treaty verification, AI/ML assurance at scale, anti-proliferation mechanisms, and more.

Our efforts are possible thanks to our supporters from Open Philanthropy, the William and Flora Hewlett Foundation, the Patrick J. McGovern Foundation, the Public Interest Technology University Network, anonymous donors, and Georgetown University. This generous support has allowed CSET to build a unique capability (and the requisite infrastructure) that allows our researchers to pursue the important topics without the constraint of short-term contracts.

I am deeply grateful to policymakers, decision makers, and thought leaders throughout government, industry, and academia within the United States and around the world who have taken the time to share their views and concerns, helping us focus on a relevant set of analytic problems. CSET is significantly stronger and more impactful thanks to these thought-provoking, relevant, and challenging questions.

Thank you for your interest in the intersection of emerging technology and security, and I hope you enjoy this report!

TIMELINE

JAN 2019: CSET founded

FEB 2019: Public launch, including website launch and $55M founding grant

SEP 2019: CSET's first papers published, synchronously with CSET co-hosting the Kalaris conference

JAN 2020: CyberAI launched

MAY 2020: 200th briefing for policymakers

SEP 2020: 50th piece of analysis published

FEB 2021: Founding Director Jason Matheny appointed to White House post

JULY 2021: Dewey Murdick announced as Director

AUG 2021: Biotech program launched

AUG 2021: New round of funding announced, total >$100M through 2025

POLICY IMPACT

CSET has established itself as a leader in understanding the implications of emerging technology for global security and in helping to shape policy responses in Washington and beyond. This work contributes to legislation, influences executive branch actions, and is widely cited by other organizations.

"

When I was the Deputy Assistant Secretary of Defense for Research, it was simply impossible to understand what the true state of the art was in all emerging tech areas of importance quickly enough to be useful. At CSET, I had more data, analytic ability, and context at my fingertips than I did within the Pentagon. CSET has collected, curated and maintained the data, infrastructure and expertise required to do this, the difference is stunning."

MELISSA FLAGG
FORMER SENIOR FELLOW

- **CSET RESEARCH HAS BEEN CITED** in reports by the White House, the National Security Commission on Artificial Intelligence, the Senate Foreign Relations Committee, Congressional Research Service, the American Association for the Advancement of Science and think tanks including the Brookings Institution and the Center for a New American Security (CNAS).

- **ON REQUEST FROM CONGRESS,** CSET experts provided advice on provisions of the FY 2021 Intelligence Authorization Act, the FY 2021 National Defense Authorization Act, and the FY 2022 NDAA that became law.

- **OTHER CONGRESSIONAL REQUESTS** have resulted in recommendations from CSET for the CHIPS for America Act, the U.S. Innovation and Competition Act, and proposed legislation still in draft form.

- **CSET EXPERTS HAVE BEEN INVITED A DOZEN TIMES TO BE WITNESSES** at congressional hearings, including before the Senate and House intelligence committees, the Senate Foreign Relations Committee, and the House Budget Committee.

- **CSET EXPERTS HAVE BEEN ASKED TO BRIEF** the Pentagon's Joint Artificial Intelligence Center, the Under Secretary of Defense for Research and Engineering, and officials with the Department of Homeland Security, the Department of State, the Commerce Department's Bureau of Industry and Security, officials in the Intelligence Community, and others across the U.S. government.

- **AND CSET HAS PROVIDED FORMAL RESPONSES** to federal government requests for information on a range of topics, including nonimmigrant student visas for the Department of Homeland Security, semiconductor supply chain risks for the Department of Commerce, and the newly-established National AI Research Resource for the White House Office of Science and Technology Policy and the National Science Foundation.

STAFF PROFILE

While earning a master's degree in Security Studies at Georgetown, **TINA HUANG** came to CSET in 2019 as a research analyst. "I was excited to be part of this new and growing organization, but didn't expect the many ways the experience would open up my horizons," she notes. Tina focused on the U.S. AI workforce and the strategic implications of military use of AI. Her publications included "Immigration Policy and the Global Competition for AI Talent," which found that certain U.S. immigration policies might be undermining the country's ability to attract and retain AI researchers and developers from overseas. Through CSET's congressional fellowship program, she served in the office of a key member of Congress with a leadership role in AI issues. She became the policy program manager with the Stanford Institute for Human-Centered Artificial Intelligence in mid-2021. "Thanks to CSET, I strengthened my grasp of cutting-edge issues in technology and global security and took part first-hand in the policymaking process," she says. "The knowledge, contacts and friendships I developed there were valuable beyond words. And it was amazing to see legislation emerge from my work!"

Talent flows and high-skill immigration

THE CRITICAL ROLE OF HUMAN CAPITAL IN AI COMPETITIVENESS is a topic that CSET prioritized from the beginning. Initially, we focused on how immigration policy affects top AI talent from around the world —and how that, in turn, affects U.S. technological competitiveness. Human capital is a crucial element in the AI ecosystem, so ensuring that the United States can attract and retain as many talented scientists and engineers as possible is a necessary component of any strategy for technological competitiveness.

CSET's research on international talent has produced both empirical findings and proactive policy recommendations. On the empirical side, one important finding is just how many international students who complete AI-relevant PhDs in the United States end up staying in the country over the long term, with more than 90 percent remaining during the year after graduation and more than 80 percent still present five years later. Similar trends are seen in the U.S. semiconductor workforce, another area CSET researchers have studied.

CSET's work has identified and highlighted a wide range of possible improvements to federal immigration law, ranging from regulatory and administrative changes, which could be made using executive branch authority, to more sweeping changes that Congress could enact.

This work has seen significant uptake by both the Trump and Biden administrations, as well as in broader conversations about technology and national security, where the centrality of STEM immigration is now much more widely acknowledged than in the past. For example, CSET's semiconductor workforce research was cited extensively in a June 2021 White House report on semiconductor supply chains. ■

LEARN MORE >

AI workforce

CSET'S RESEARCH ON THE U.S. AI WORKFORCE considers the entire domestic talent pipeline and expands beyond the most elite talent to consider the full spectrum of AI occupations and training. This work helped us build the conceptual and empirical scaffolding needed to have grounded, data-driven conversations about the AI workforce and AI education in the United States. Understanding

CSET TWEET

Center for Security and Emerging Technology ✓
@CSETGeorgetown

🎉 New Policy Brief 🎉

In our new report, produced in collaboration w/ @MITREcorp, authors @dianagcarew, Ron Hodge, @Luke_Koso, Kayla Goode & Jonathan Rotner provide 15 ideas on how @DeptofDefense can leverage its hidden cadre of #AI talent. Read more:

September 2021

The DOD's Hidden Artificial Intelligence Workforce: Leveraging AI Talent at the U.S. Department of Defense

Diana Gehlhaus, Ron Hodge, Luke Koslosky, Kayla Goode and Jonathan Rotner

CSET and MITRE Policy Brief

cset.georgetown.edu
The DOD's Hidden Artificial Intelligence Workforce - Center for Security and E...
This policy brief, authored in collaboration with the MITRE Corporation, provides a new perspective on the U.S. Department of Defense's struggle to recruit and ...

7:04 AM · Sep 28, 2021 · Twitter Web App

RETWEET

BY LT. GEN. JACK SHANAHAN
Inaugural Director of the U.S. Department of Defense Joint Artificial Intelligence Center

Jack Shanahan
@Fermat15

Good news: there's more AI talent in DoD than you think. Bad news: it's not being used as effectively as it should be (sound like early cyber?). Excellent recommendations on how @DoDJAIC can play a lead role in orchestrating better AI personnel policy/talent mgmt across Services.

Center for Security and Emerging Technology ✓ @CSETGeorge... · Sep 28
🎉 New Policy Brief 🎉
In our new report, produced in collaboration w/ @MITREcorp, authors @dianagcarew, Ron Hodge, @Luke_Koso, Kayla Goode & Jonathan Rotner provide 15 ideas on how @DeptofDefense can leverage its hidden cadre of #AI talent. Read more: cset.georgetown.edu/publication/th...

7:28 AM · Sep 28, 2021 · Twitter Web App

what the AI workforce really looks like—including the scale, geographic distribution, and wide variety of skills and qualifications at play—is key to making informed policy on AI education and workforce development.

CSET's workforce research has also focused on technology talent competition with China. This work has included assessments of U.S. visa restrictions on Chinese students and researchers, and comparative studies of STEM and AI education in China and the United States. Since the mid-2000s, China has consistently graduated more STEM PhDs than the United States, a key indicator of a country's future competitiveness in STEM fields. CSET explored the data on STEM PhD graduation rates and projected their growth over the next five years, during which the gap between China and the United States is expected to increase significantly. Other CSET research compared efforts to integrate AI education in China and the United States, advantages and disadvantages of the U.S. approach to AI education, and implications for national security.

A globally competitive AI workforce hinges on the education, development, and sustainment of the best and brightest AI talent. CSET research identified the need for a clearly defined artificial intelligence education and workforce policy in the United States, and provided recommendations designed to grow, sustain, and diversify the U.S. AI workforce. These recommendations are designed to leverage opportunities within the U.S. education and training system while mitigating its challenges, and to prioritize equity in access and opportunity to AI education and AI careers. ◼

READ CSET AI WORKFORCE RESEARCH >

CSET TRANSLATIONS
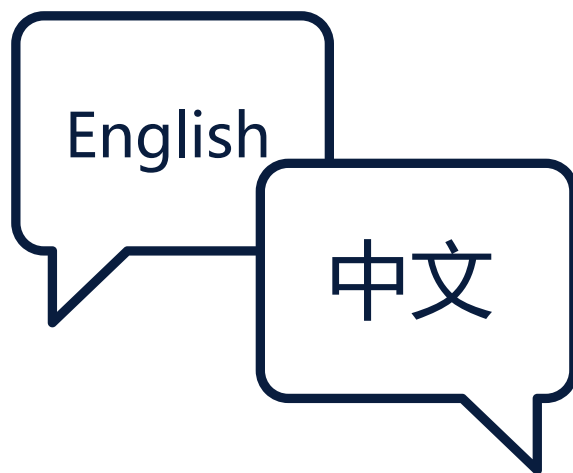
Too often, analyses of international technological capabilities or plans are hindered by the "soft encryption" of foreign language materials. CSET maintains an on-demand translation function, which allows both CSET analysts and external stakeholders to request professional translations of documents of interest.

So far, CSET has produced 357 translations of key strategic, policy, and technical documents from China and Russia, 118 of which are publicly available on our website because they are not under copyright restrictions. Major examples include China's 14th Five-Year Plan, Russia's AI strategy, and a series of articles describing 35 "stranglehold" technologies that China is unable to produce domestically.

CSET's translation capability, which is unique among our peer organizations, both informs our own analysis and serves the broader technology and national security community. Translations of Chinese-language documents powered CSET publications and data interactives on topics from State Council budgets and government guidance funds to tracking talent programs and China's wish list of foreign technologies.

In the summer of 2021, a bipartisan group of legislators introduced a bill to establish an Open Translation and Analysis Center, with exactly the same reasoning that drives CSET's translation work. We see this proposal as a vindication of our model, and would be delighted for our translation function to complement such a center.

OECD COLLABORATION

The Organisation for Economic Co-operation and Development adopted the first intergovernmental standard on AI, the OECD AI Principles, in May 2019. CSET was invited to join the OECD Network of Experts on AI (ONE AI) and to share its expertise with the nascent OECD Policy Observatory, which facilitates dialogue between stakeholders on AI matters while providing multidisciplinary, evidence-based policy analysis.

CSET has been closely involved in the ONE AI working group on the Classification of AI Systems. This working group was tasked with developing a framework to help policymakers as well as system operators and developers efficiently identify, monitor, and characterize AI systems in development or use, and determine which AI systems are higher risk and warrant greater policy attention. CSET also designed a study to test the framework's usability and compare performance with other potential frameworks. CSET published a paper outlining this work, and a version of the framework developed by the OECD will be published in coming months.

STAFF PROFILE

After a career as a technology lawyer, **SAIF M. KHAN** joined CSET in 2019 hoping to combine that experience with his interest in the impact of emerging technologies on society and the security policy landscape. "Technologies like artificial intelligence will pose immense challenges and opportunities for the world in the coming years, and I wanted to translate what I learned working in the technology and legal sectors into policy work that ensures the adoption of these technologies goes well," he says. He took note early on that the availability of one technology in particular was key to the international competition in the development of AI: semiconductors. His reports for CSET on the subject were featured in The Financial Times, The Washington Post, Fortune and other outlets. "CSET is unique in Washington: I can't imagine any other place that could have better provided the resources, time, and support I needed to conduct deep, data-driven research on technology policy," he says. "Turning that knowledge into actionable information for high-level decision-makers has been gratifying and a great honor." A specialist in semiconductor supply chains and related U.S. policy, who has testified before the Senate Foreign Relations Committee, Saif is currently detailed to the National Security Council under an arrangement whereby U.S. university personnel can serve in federal agencies.

Semiconductor supply chains

FROM THE VERY BEGINNING, THE CSET TEAM IDENTIFIED ADVANCED SEMICONDUCTORS—the computer chips that power AI systems—as a high priority for analysis. Although semiconductors are central to the future of AI, in 2019 shockingly little research existed that explored their strategic relevance in a national security context.

Since then, CSET has published more than 10 analyses of semiconductor supply chains, covering ground from the basics of how semiconductors power cutting-edge AI, to the sector's unique supply chain dynamics, to the importance of foreign talent in the U.S. semiconductor workforce. Our work on this topic has been uniquely impactful because we have been able to dig into the technical and economic details of these incredibly complex supply chains while maintaining a focus on the high-level strategic importance of the issue. No one else has combined as much depth and rigor with a focus on presenting findings and policy recommendations in plain language.

Key findings and recommendations of this work include:

- While China has invested heavily in its domestic semiconductor manufacturing industry, it remains dependent on the United States and U.S. allies and partners for key inputs, including semiconductor manufacturing equipment—most notably advanced photolithography machines. A multilateral approach is the only way to create effective controls in this area. Depending on what is being controlled, the United States must partner closely with Taiwan, South Korea, Japan, the Netherlands, the UK, Germany, and others in order to create the desired effect.
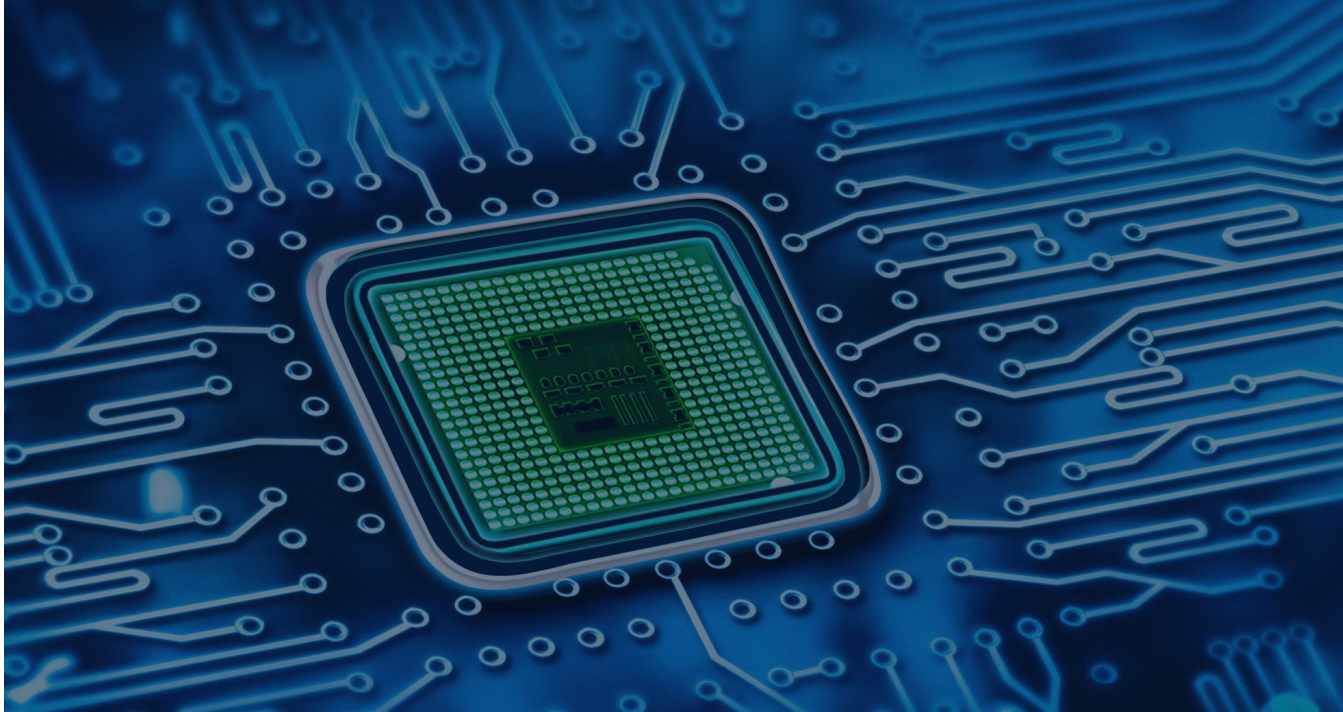
- Measures to protect U.S. innovation should be paired with a strategy to promote domestic semiconductor manufacturing advances, including via onshoring incentives, investments in long-term research and development, and talent pipeline development.

These findings and recommendations have enjoyed wide reach, including being incorporated into the CHIPS for America Act (passed into law as part of the 2021 National Defense Authorization Act) and contributing to the final report of the National Security Commission on AI. More generally, semiconductors have become much more central in discussions of national security and emerging technologies, which we believe is long overdue.

CSET's success in this area was enabled by several factors. Because we have the freedom to focus on topics our experts identify as significant and likely to have an impact, we are able to jump into areas that are not yet widely recognized as strategically consequential and lead the conversation in important directions. Being able to sustain a multi-year research program allowed us to go deep on this complex topic, developing in-house expertise on both the subject matter and the policy environment surrounding it. Our data team and data infrastructure also made it possible for us to draw on proprietary data to reach our conclusions. ◼

VIEW CSET SEMICONDUCTOR WORK >

STAFF PROFILE

CINDY MARTINEZ came to CSET with experience in advising senior officials at the Department of Homeland Security (DHS) on technology policy, including offensive and defensive cyber operations and space security issues. "The pace of national security policymaking can be punishing, leaving little room to personally indulge in the latest advancements or quality research in your field," she observed. "I reached a point in my career where I wanted to obtain a better grasp on emerging technology, ensuring that my future work is based on a sound understanding of its capabilities, benefits, and limitations. This is what led me to apply at CSET." When she joined CSET's CyberAI project as a semester research analyst, Cindy was earning a master's degree in Security Studies at Georgetown. While at CyberAI, she had an immediate impact through co-authoring a report, "U.S. Demand for Talent at the Intersection of AI and Cybersecurity." Her previous experience with DHS helped ensure that the team's work stayed policy-relevant. Cindy also wrote an op-ed about how the U.S. government could address its workforce talent issues and increase youth recruitment in the cybersecurity and artificial intelligence fields. She now works as a policy analyst for the Department of Defense's Joint Artificial Intelligence Center, showing a remarkable ability to transition from government to an academic setting and back again.

CyberAI

THE CYBERAI PROJECT AT CSET IS FOCUSED ON ISSUES AT THE INTER-SECTION OF CYBERSECURITY AND AI. The project launched in January 2020 with generous support from the William and Flora Hewlett Foundation. CyberAI's work covers topics ranging from technical analysis of machine learning vulnerabilities to primers for policymakers to open-source investigations. Early research focused on broad investigations of the potential of AI to alter cyber operations. These reports sought to provide policymakers with a baseline of AI's present impact and highlighted important areas for future research, which the team has continued.

One major theme is understanding how advances in AI and machine learning will change cyber operations, both in offense and defense. CyberAI's work on this has combined technical grounding with a strategic view, contextualizing the potential for AI innovation within the larger history of traditional automation and statistical tools in cybersecurity. This kind of analysis orients policymakers to areas that may see important changes, while cutting through the hype that often surrounds these discussions.

In some cases, the CyberAI team goes so far as to directly demonstrate new AI capabilities and weaknesses with implications for cybersecurity. One groundbreaking report tested how well GPT-3, a leading-edge AI text

generation system, could produce disinformation; this analysis found that GPT-3 could generate text that was effective for a range of disinformation-related tasks, especially when used as part of a human-machine team. Other CyberAI work has highlighted the security vulnerabilities of AI systems and the shared resources they rely on that make them vulnerable to new types of hacking or manipulation.

Additionally, CyberAI research has examined the geopolitical landscape by considering how AI could alter competition and how nations are pursuing AI capabilities. For example, the project has explored China's cyber and AI ambitions and specific efforts underway within the country. This research has included an exploration of academic work across China, as well as an interactive, map-based deep dive into the newly established National Cybersecurity Center in Wuhan.

As is true across all of CSET, CyberAI strives to combine a strong understanding of the technologies at hand with a high-level picture of their strategic and policy relevance, and to blend analytic rigor with clear writing and practical takeaways. This approach allows us to produce grounded, insightful contributions that inform policymakers and support better policy decisions. ■

VIEW THE CSET CYBERAI PROJECT >

PUBLIC RESEARCH RESOURCES

CSET has provided a number of valuable public resources—including expansive datasets, translations of primary source documents, and data visualizations—that enable policymakers and researchers alike to cut through speculation and access the information they need.

- **THE CHINESE TALENT PROGRAM TRACKER** catalogues publicly available information, including primary sources such as translated Chinese government documents, about China's party- and state-sponsored talent programs that recruit researchers—Chinese citizens and non-citizens alike—to bolster its strategic civilian and military goals.

- **THE CHINESE STATE COUNCIL BUDGET TRACKER** compiles publicly available information about the budgets of more than two-dozen high-level Chinese government entities, including those that support science, technology, and talent recruitment.

- **THE PRIVATE-SECTOR AI-RELATED ACTIVITY TRACKER (PARAT)** collects data related to companies' AI research and development to inform analysis of the global AI sector.

- **THE NATIONAL CYBERSECURITY CENTER MAP** (see image above, pages 16 and 17) uses satellite imagery to offer a closer look at the sprawling 40 km² campus of China's National Cybersecurity Center in Wuhan.
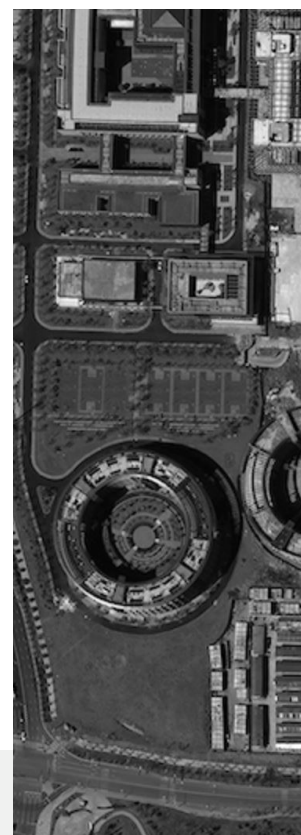
■ **THE CSET LEGISLATION TRACKER** serves as a resource to identify and monitor U.S. federal legislation related to emerging technology and national security. The tracker includes identifying information for each piece of legislation, links to related CSET analyses, and access to associated congressional hearings, among other items.

■ **THE MAP OF SCIENCE**—built on a rich interlinkage of multiple datasets of scholarly literature—groups scholarly literature into clusters according to their citation linkages and then color-codes them based on their high-level research area.

■ **TRANSLATIONS** of key strategic, policy, and technical documents from China and Russia are shared publicly whenever copyright allows it.

Map of Science

IN OCTOBER 2021, WE LAUNCHED OUR MAP OF SCIENCE AS AN ONLINE INTERACTIVE TOOL. The Map is constructed by grouping scholarly literature into clusters, according to citation linkages, and then displaying these clusters by color according to high-level research area and arranged according to citation pattern.

One of CSET's founding premises was that having an accurate picture of the scientific and technological landscape is a prerequisite to developing wise policies and strategies for emerging technologies. The tight integration of data science and open-source data into our research model reflects this premise, and the Map of Science is a vivid example of the fruit this approach can bear. Although the final product may look deceptively simple, it reflects many years of insight and elbow grease from data scientists, annotators, analysts, a web developer, and many others. The Map is not built on a single dataset, but rather on a rich interlinkage of multiple datasets of scholarly literature. Data team contributions that made it possible to create the Map include the development of CSET's merged corpus (which combines and deduplicates hundreds of millions of scientific articles from six different source datasets in multiple languages), organizational entity resolution (that is, unifying the representation of organizations that appear under multiple names), CSET's AI classifier (used to identify and categorize AI papers), and a range of ongoing collaborations with external researchers and organizations to make use of the best available methods for clustering scholarly research and forecasting growth.
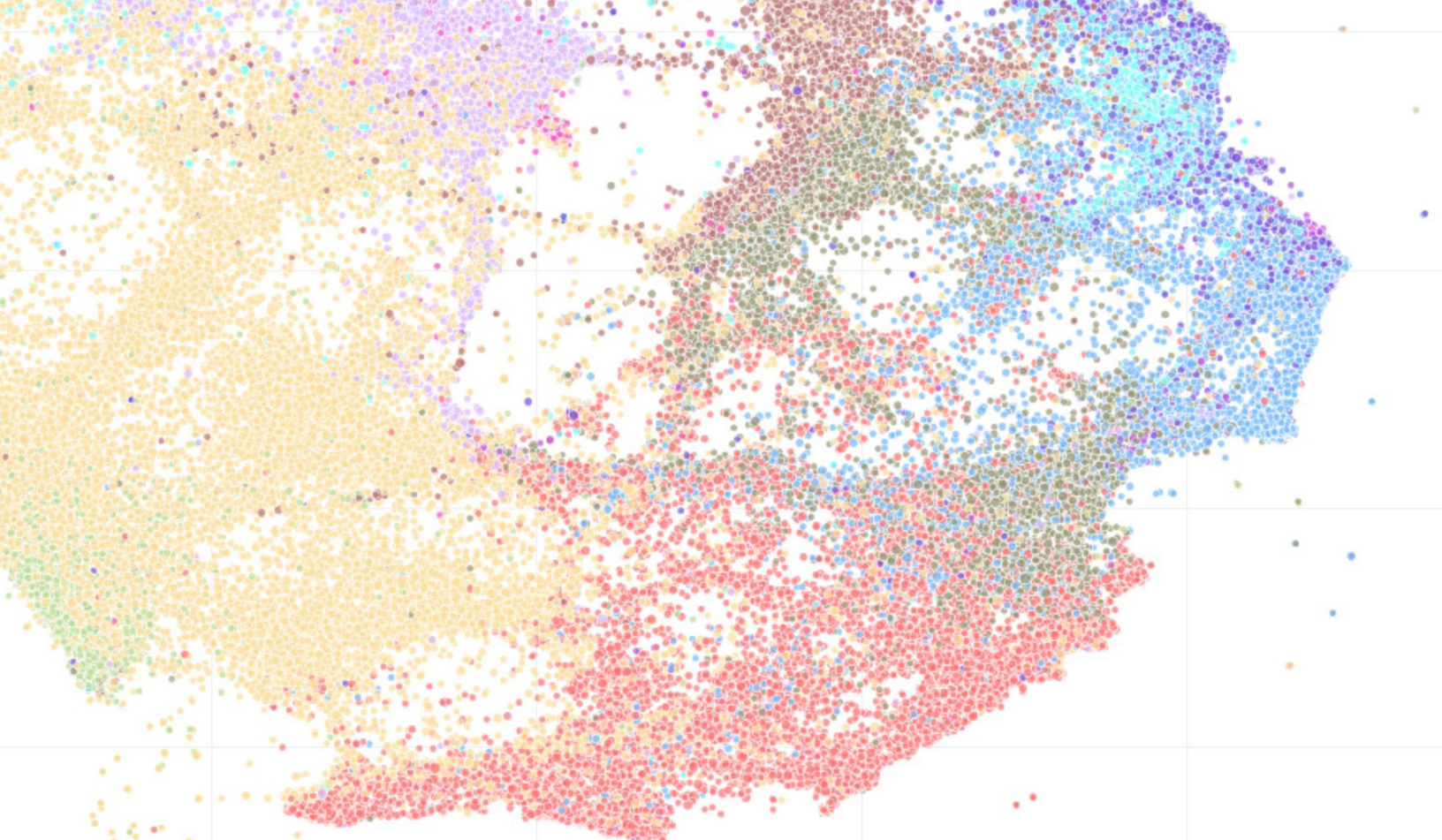
The result is a multi-purpose tool that can facilitate broad-based or specific analyses of the research literature in any emerging (or established!) technology area. The Map makes it possible to get an empirically grounded view of what is going on in the research landscape. This can include analyses that take a bird's-eye view, such as looking at clusters that have grown rapidly in recent years, as well as investigations of particular topics of interest. CSET analyses leveraging the Map of Science have looked at sub-areas of AI (such as computer vision, natural language processing, and robotics), the development of AI for surveillance, progress in AI safety, and compared country research output.

The Map and the underlying enriched datasets of scientific research publications can also be used in tandem with other sources of information, including data on investments, patents, and job postings. CSET's Private-sector AI-Related Activity Tracker (PARAT), for instance, draws on the merged corpus and other data to allow users to explore private-sector companies that are active in AI research and development. We plan to expand our use of the Map of Science and continue developing new data resources into the future. ◾

CSET IN THE MEDIA

CSET experts and their work have earned the attention of prominent news media, garnering more than **470 media mentions**, including:

THE NEW YORK TIMES

TOPIC: TALENT

The New York Times cited an issue brief by Remco Zwetsloot, Jacob Feldgoise and James Dunham in an article emphasizing how Chinese nationals studying AI are likely to remain in the United States and could be the key to advancing U.S. AI talent. According to their brief, "through 2018, nine out of 10 Chinese nationals who completed doctorate degrees stayed for at least five years after graduation."

AXIOS

TOPIC: CYBER

Axios Future featured CSET's report, "Truth, Lies, and Automation," where experts Ben Buchanan, Andrew Lohn, Micah Musser and Katerina Sedova examined the capability of OpenAI's AI system GPT-3 ability to potentially fuel automated disinformation campaigns.

FORTUNE

TOPIC: ALLIANCES

To understand India's AI capabilities, Fortune spoke with CSET Research Analyst Husanjot Chahal about her data brief "Mapping India's AI Potential," coauthored with Sara Abdulla, Jonathan Murdick and Ilya Rahkovsky. Rather than viewing India as a competitor, Chahal described the ongoing AI relationship between India and the United States as "an avenue of cooperation."

WIRED

TOPIC: SEMICONDUCTORS/CHIPS

CSET Research Analyst Will Hunt spoke with Wired to address how U.S. government investment in domestic fabrication for chip manufacturing can improve the U.S. chip shortage. Hunt offered further recommendations to advance the U.S. semiconductor industry in his testimony before the Strategic Technologies and Advanced Research (STAR) Subcommittee.

NATIONAL DEFENSE

TOPIC: SAFETY

National Defense reached out to CSET's Director of Strategy Helen Toner to discuss AI failures and how military systems can build safe and trustworthy AI from her and Zachary Arnold's policy brief "AI Accidents: An Emerging Threat."

THE WASHINGTON POST

TOPIC: CHINA

CSET Research Analyst Ryan Fedasiuk spoke with The Washington Post about U.S. investments in Chinese companies with military ties, based on the report "Harnessed Lightning" that he wrote with Jennifer Melot and Ben Murphy. "It's clear there are large gaps in the U.S. export control system that allow the Chinese military to access equipment, information and capital originating in the United States," Fedasiuk said. "But plugging these gaps is easier said than done."

And opinion pieces by CSET authors have been published in dozens of publications, among them The Wall Street Journal, Foreign Affairs, and Scientific American.

READ MORE OF CSET IN THE NEWS >

A clear-eyed view of China

CHINA'S INCREASING TECHNOLOGICAL CAPABILITIES HAVE ENORMOUS RELEVANCE TO ANY DISCUSSION OF TECHNOLOGY AND NATIONAL SECURITY. But too often, policy discussions—especially in open-source contexts—are based on an incomplete or inaccurate picture of what China's plans, achievements, and capabilities actually are. Sometimes this means downplaying and underestimating the truth; other times, it means hyping or overstating the threat. If strategic competition with Beijing is to be a major thrust of U.S. policy in the coming decades, it will be essential to have an accurate and nuanced understanding of what is actually happening—and not happening—in China.

Accordingly, a substantial amount of CSET's work has been dedicated to illuminating the actual situation regarding China's technological development. We make use of a wealth of unclassified data sources, including Chinese government documents, bibliometric data, investment data, surveys, and other sources, to provide grounded, in-depth assessments. Many of these sources are available only in Chinese, and CSET often translates these for the first time into English. Sometimes, this work makes it possible for policymakers to talk openly about information that had previously been discussed only in classified spaces and/or unavailable to non-Chinese speakers; at least as often, our analysis breaks new ground altogether.

"

CSET's work on Chinese AI was frequently cited in DoD meetings. The work cut through a lot of hype and otherwise overblown concerns—'according to CSET China is not 10 feet tall.' There were no alternative sources that would have given equivalent insights regarding Chinese AI within or outside the U.S. Government."

DR. MARK LEWIS
FORMER DIRECTOR OF DEFENSE RESEARCH & ENGINEERING, DEPUTY
UNDERSECRETARY OF DEFENSE (ACTING), OFFICE OF THE SECRETARY OF DEFENSE

Notable CSET publications along these lines cover a range of topics. In 2019, we published an analysis of China's annual spending on AI R&D, finding that although it was difficult to pin down an exact number, an estimate that had been circulating in Washington of $70 billion per year was likely an order of magnitude too high; this analysis was later cited by the White House. In 2021, we published a major report on what Chinese diplomatic documents tell us about China's technological wish list, analyzed what Sino-Russian technological cooperation looks like in practice, and released online interactive tools that delved into Chinese talent plans and government budgets, and we have published deep dives into China's technology acquisition institutions and practices. These publications were designed to cut through hype, raise new concerns, or both. What they all have in common is that they draw on data and evidence to counter misunderstandings and add nuance. ■

VIEW CSET ANALYSIS ON CHINA >

FORETELL

Foretell is a crowd forecasting platform, incubated by CSET, that gathers and synthesizes forecasts on questions related to technology and national security.

The platform, developed in partnership with Cultivate Labs, takes big-picture questions of interest to policymakers and breaks them down into specific, forecastable indicators. This approach is borne out by research showing that the wisdom of the crowd can outperform expert judgment, even on geopolitical topics where experts have access to classified information.

Since being established in mid-2020, Foretell has hosted more than 27,000 forecasts on 113 questions, with contributions from nearly 2000 individual forecasters.

CSET blazed a trail in this field by creating novel capabilities such as question aggregation and a new type of fusion between data and forecasting. CSET is preparing to transition Foretell to a policy-focused home that will continue to nurture and expand on this platform.

VISIT THE FORETELL PLATFORM >
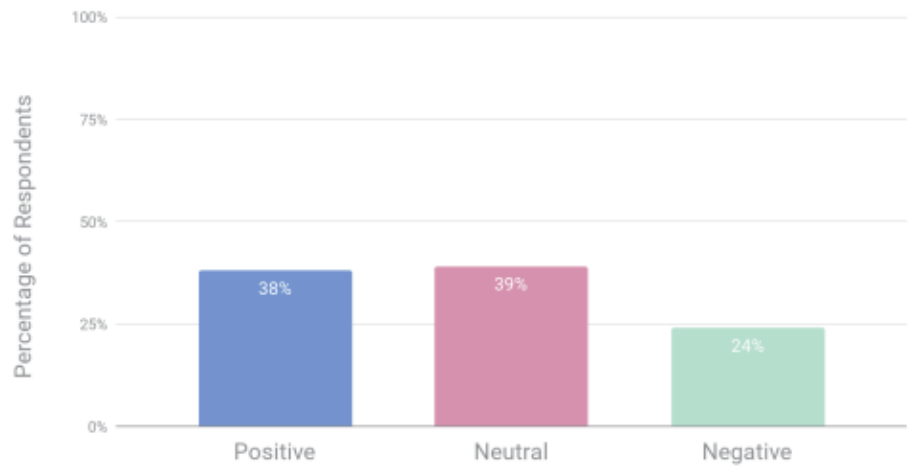
CSET SURVEYS

CSET has deployed nine original surveys and published eight reports with findings from this unique data.

Each of these surveys was designed in-house, approved by Georgetown's Institutional Review Board, and distributed to answer questions posed by CSET researchers. In each case, our survey analyst and data team worked closely with researchers to design a survey, develop a sampling frame, distribute the survey, analyze responses, and present findings.

CSET's first surveys, fielded in 2019, included a questionnaire for foreign diplomatic representatives to understand their countries' priorities for international AI collaboration and a survey of U.S. AI PhDs to learn about their career preferences and paths. Drawing on CSET's translation capabilities, in early 2020 we fielded a survey of Chinese researchers; later that year, we asked AI industry professionals about their views on working with the U.S. Department of Defense.

More recently, CSET designed a survey experiment to assess the persuasiveness of machine-generated misinformation, with results published in Truth, Lies, and Automation and highlighted by Wired. Results from another CSET survey experiment testing the usability of several versions of an AI systems classification framework were published in "Classifying AI Systems."

In addition to surveys, CSET has carried out several interview projects, including interviewing personnel to understand Department of Defense processes for identifying and leveraging its AI workforce. As we enter our fourth year, we have several new survey projects in the works!

PARTNERING WITH GEORGETOWN UNIVERSITY

CSET is proud to have been founded under the aegis of Georgetown's Walsh School of Foreign Service, and our partnership has produced many benefits.

Several CSET senior fellows serve as adjunct SFS faculty, while other team members have taught skill-building workshops and held brown-bag professional sessions for graduate and undergraduate students. More than 45 students have served in multiple roles, and some have been credited as co-authors on published reports. SFS faculty, serving as CSET Faculty Fellows, have contributed to CSET publications. And CSET's ongoing collaboration with Georgetown's Tech & Society Initiative became even closer in late 2021 when we joined other T&S initiatives in our purpose-built offices in a newly-acquired building that expands Georgetown's presence near the U.S. Capitol.

STAFF PROFILE

When **DARRIN GLADMAN** started with CSET as a semester research analyst in the fall of 2020, he was hoping "to put theoretical knowledge into practical use, particularly identifying business problems and the best strategies to address those issues." He teamed up with one of our senior fellows and supported research tasks such as analyzing data, completing literature reviews, and developing visualizations that offered insights into government investment in patents and AI. Darrin also worked closely with CSET's data science team to apply language models to extract information from AI/ML research literature. He went on to become a data scientist for Booz Allen Hamilton, a consulting firm well known in Washington, DC circles. "Overall, CSET's internship program helped build my technical and interpersonal skills," Darrin says. "These skills are used today in my career. I could not be more thankful."

FUTURE DIRECTIONS

In its first three years of existence, CSET has explored a broad span of issues relating to the national security impacts of AI, advanced computing, cybersecurity, and emerging technologies more generally. In 2022 and beyond, several lines of research seeded in 2021 will expand and grow, including:

BIOTECHNOLOGY: Where is potentially risky research taking place around the world? How should the governance of dual-use research and new therapy development be approached? Will advances in AI impact discovery in biotechnology, especially genomics? How can policymakers support the bio-economy, including considerations of supply chains, innovation infrastructure, and research security?

ASIA-PACIFIC: How are AI and other emerging technologies developing in the Asia-Pacific region? How do different countries' capabilities and priorities bear on U.S. relationships with the region?

TESTING AND STANDARDS: When do AI systems work well, and when do they fail? How can these failures be predicted, prevented, or mitigated? What is needed to move towards a world where stakeholders are better prepared to test and benchmark AI systems, from early design and development stages through operational testing and deployment?