Dr. Amy Zegart
Morris Arnold and Nona Jean Cox Senior Fellow, Hoover Institution
Chair, Artificial Intelligence and International Security Steering Committee, Stanford University
Professor of Political Science, by courtesy, Stanford University

Intelligence Community Reform with Think Tank Leaders
Open Hearing of the House Permanent Select Committee on Intelligence
February 28, 2023

Opening Statement for the Record

Mr. Chairman, Ranking Member Himes, distinguished Members of the Committee, thank you for inviting me today. It is an honor to be with you. America's intelligence agencies perform an essential mission, and they are facing unprecedented challenges in today's technological age. This committee's oversight is crucial to their success and the security of the nation.

I have spent thirty years researching American intelligence agencies. My newest book, *Spies, Lies, and Algorithms,* examines how emerging technologies are transforming the global threat landscape and the ability of our intelligence agencies to understand it. **To summarize my findings in a sentence: This is an adapt-or-fail moment. Emerging technologies are profoundly disrupting the intelligence enterprise by generating what I call the "The 5 Mores": More threats to track, more speed at which intelligence must move, more data to analyze, more customers who don't have security clearances or work in the U.S. government, and more intelligence competitors.** Although American intelligence agencies are taking important steps to rebalance resources and refocus from counterterrorism to great power competition, those changes will not be enough. Without more far-reaching reforms, especially in science and technology work force recruitment and the use of open-source intelligence (OSINT), the U.S. Intelligence Community (IC) will fall behind.

My remarks cover three points:

- What makes this technological moment unique
- How emerging technologies are challenging intelligence
- What to do about it: The need to improve science and technology work force recruitment and create a new open-source intelligence agency

What Makes This Technological Moment Unique

Technology is always changing, but this moment is different. Never have so many technologies changed so much so fast at the same time. Internet connectivity has skyrocketed from less than one percent of the world's population in the 1990s to two thirds of the world today. Artificial intelligence is disrupting nearly every industry, from the military to medicine. Some estimate

that AI could eliminate up to 40 percent of jobs worldwide in the next 25 years. Commercial satellite capabilities have increased dramatically, offering low-cost eyes in the sky for anyone to detect events unfolding on Earth. Already more than 5,000 satellites orbit the planet, with thousands more commercial satellites estimated to be launched in the next decade. Quantum computing could eventually unlock the encryption protecting nearly all the world's data, making even highly classified documents available to enemies. Synthetic biology is enabling scientists to engineer living organisms, paving the way for what could be revolutionary improvements in the production of food, medicines, data storage, and weapons of war.

Understanding the promise and perils of these and other emerging technologies is a vital intelligence mission. Policymakers need to know, for example:

- Will the U.S. or China win key technological competitions? What are the likely effects?
- How will future wars be fought and won?
- How could new technologies address global challenges such as climate change?
- How could adversaries use data and new technologies to coerce, commit atrocities, evade sanctions, develop weapons, undermine democracy, and secure advantages that harm American interests, threaten our freedoms, and endanger our citizens?

Answering these questions is getting harder because the landscape of American innovation has flipped. Technological breakthroughs like GPS and the Internet used to be invented by U.S. government agencies and later commercialized by the private sector. Today, technological innovations are more likely to be invented in the private sector, where they are developed by a multinational work force, funded by foreign investors, and sold to global customers.

Power isn't just shifting abroad. Power is shifting at home. In the past, the sources of national power were tangible assets like territory and military might that were controlled by governments. Increasingly, however, the sources of national power are intangible assets like data and technology that are controlled by the private sector. American companies are developing capabilities that can be used by enemies they cannot foresee with consequences they cannot control. Meanwhile, the Pentagon and Intelligence Community are struggling to adopt commercial technologies at the speed of invention instead of the pace of bureaucracy.

Emerging Tech's "Five Mores" for Intelligence

Emerging technologies are challenging U.S. intelligence agencies in five ways.

More threats

Technology is making the global threat list longer and harder to manage. For centuries, countries protected themselves by building powerful militaries and taking advantage of good geography. But in cyberspace, anyone can attack from anywhere. Small attacks can add up to strategic consequences. Cyber weapons can be used by the weak, not just the strong. And the

U.S. is simultaneously powerful and vulnerable because we rely on digital systems and because our freedom of speech makes it possible for enemies to wage influence operations at scale.

More speed

Emerging technologies are also accelerating the speed at which intelligence must move. In the 1962 Cuban Missile Crisis, President John F. Kennedy had 13 days to assess intelligence and decide on a course of action. On September 11, 2001, President George W. Bush had just 13 hours after the first plane crashed into the World Trade Center to review intelligence and announce a response. Today, the time for presidents to consider intelligence before making major policy decisions is closer to 13 minutes or 13 seconds. As GEN. Paul. M. Nakasone noted in a recent public speech, "the world has moved to an era where the shift from competition to crisis to conflict can occur in weeks or days or even minutes rather than years." Satisfying a policymaker's need for timeliness while carefully collecting, vetting, and assessing intelligence is a delicate balance that is growing more challenging.

More data

Intelligence analysts are drowning in data. Every second, the Internet transmits about a petabyte of data. That's equivalent to the information a person consumes binge-watching movies nonstop for over three years. In 2018, the Intelligence Community was capturing more than three NFL seasons' worth of high-definition imagery a day on each sensor deployed to a combat theater. In 2020, one soldier deployed to the Middle East was so concerned about the crushing flow of classified intelligence emails he was receiving, he decided to count them. The total: 10,000 emails in 120 days.

The IC needs to adopt more automated analytics to help human analysts find needles in these exponentially growing haystacks as well as derive more insights from the haystacks themselves. Already, private sector companies are using AI models to predict political instability and military exercises with high accuracy based on datasets of open-source indicators.

More customers

Today, intelligence agencies must serve a wider array of customers who don't hold security clearances, command troops, or work in the U.S. government. Voters need intelligence about foreign influence operations seeking to polarize society and undermine elections. Tech company leaders and critical infrastructure executives need intelligence about foreign cyber threats to and through their systems. And American national security increasingly depends on sharing intelligence faster and better with allies and partners.

The IC is making significant progress on this front, releasing more unclassified products and engaging the outside world. The success of this strategy has been on full display in Ukraine. Declassifying intelligence warned the world about Russia's invasion, helped rally the allies behind a fast response, and raised the costs for countries like China to hide behind Putin's lies

and side with Russia. In the past year, intelligence sharing with Ukraine and other allies and partners has grown, along with the realization that national advantage can come from revealing intelligence, not just concealing it. Yet producing intelligence products for a wider set of customers is still an unnatural act for agencies used to operating in secret.

More competitors: the open-source revolution

Intelligence isn't just for government spy agencies anymore. The explosion of open-source information available online, the growth of commercial satellite capabilities, and the rise of AI have created an open-source intelligence revolution that is making new insights possible and creating a new global ecosystem of citizen-sleuths. Private individuals and groups have been tracking the Ukraine War in ways that were unimaginable in earlier conflicts. Journalists have reported battlefield developments using commercial satellite imagery. Former government officials have been monitoring on-the-ground daily events and offering over-the-horizon analysis on Twitter. A team of students at Stanford led by former U.S. Army and open-source imagery analyst Allison Puccioni has been using TikTok videos, commercial satellite thermal and electro-optical imaging, geolocation tools, and more to uncover and verify human rights atrocities committed by Russian troops in Ukraine and report them to the United Nations.

In the nuclear realm, citizen-sleuths have used open-source intelligence to uncover China's new ICBM silo fields, determine the locations of North Korea's first nuclear tests, and quickly discover that the Iranian government was lying in 2020 when it claimed a suspicious fire damaged an industrial shed under construction. The shed turned out to be a nuclear centrifuge assembly facility at Natanz, Iran's main uranium enrichment site.

This burgeoning open-source world brings significant new opportunities and risks. On the positive side, citizen-sleuths offer more eyes and ears scanning for developments and dangers. Unburdened by bureaucracy, open-source intelligence can move fast. And it can be shared without revealing sensitive sources and methods. But because citizen-sleuths don't have to answer to anyone or train anywhere, errors are more likely. Deliberate deception is, too. Increasingly American intelligence agencies will have to burn the most precious resource they have – time –fact checking and debunking the work of others. Even accurate findings can make crises harder to manage by publicizing information that backs leaders into corners and makes graceful exits and secret compromises more difficult. Open-source intelligence is also leveling the intelligence playing field – and not in a good way. In 2020, for example, Iran used commercial satellite imagery to monitor U.S. forces in Iraq before launching a ballistic missile attack that wounded more than 100 people.

Two Important Areas for Reform: Work Force Recruitment and Open-Source Intelligence

American intelligence agencies are working hard to meet these challenges, but success requires more wholesale reforms. Two important areas to consider are: (1) Re-imagining science and technology work force recruitment; (2) Creating a new open-source intelligence agency.

A new recruiting approach: wooing, not weeding

Even in the technological age, human talent is the most important ingredient for success. The Intelligence Community must recruit more officers with science and technology backgrounds to *understand* how emerging technologies are shaping the world and to *adopt and use* new technologies to improve collection and analysis. It also needs to win more hearts and minds in the private sector.

Intelligence agencies see the people who join their ranks. At Stanford, I see the ones who got away. There is a significant missed opportunity, especially with engineering students. Intelligence recruiting is designed to weed when it should be designed to woo. Despite reform efforts, the current approach to hiring is outdated, slow, remarkably impersonal, and designed to hire employees for life. No first-rate technology company recruits talent that way. The IC needs a modern recruiting approach with a human touch that makes candidates feel valued, moves in weeks or months rather than years, and is designed to create ambassadors, not lifers -- inspiring every applicant to leave the process asking, "How can I help the IC wherever I go?"

A dedicated open-source intelligence agency

The open-source revolution is here to stay, and the Intelligence Community needs to find ways to harness its power, seize its opportunities, and mitigate its risks. Incremental changes to existing agencies are unlikely to be enough. It is time to create a new, dedicated open-source intelligence agency.

Creating a 19th agency may seem duplicative, but it is essential. Despite the IC's best efforts, open-source intelligence remains a second-class citizen because it has no agency with the budget, hiring power, or seat at the table to champion it. So long as open-source intelligence is embedded in secret agencies that value classified information more, it will languish.

An open-source intelligence agency would bring innovation, not just information, to the Intelligence Community. The agency could hire scientists and engineers without waiting for lengthy security clearances, and it could locate offices in tech hubs where engineers already live and want to stay – creating a cadre of technologists who move in and out of government more easily, increasing the IC's presence and prestige in private sector circles, and bringing a continuous stream of ideas back inside. The agency could also help the Intelligence Community adopt new collection and analysis technologies faster and better by testing them with unclassified material. And it would be ideally positioned to engage with leading open-source intelligence organizations and individuals outside of government to develop tradecraft and ethical standards and outsource more work to responsible nongovernmental partners, freeing up intelligence agencies to focus their unique capabilities on missions that nobody else can do.

Thank you, Mr. Chairman. I look forward to your questions.

Dr. Amy Zegart is a senior fellow at the Hoover Institution and the Freeman Spogli Institute for International Studies, professor of political science by courtesy, and chair of the Artificial Intelligence and International Security Steering Committee at Stanford University. She specializes in U.S. intelligence, cybersecurity, and the intersection of emerging technologies and national security. The author of five books, her award-winning research includes the leading academic study of intelligence failures before 9/11 -- Spying Blind: The CIA, the FBI, and the Origins of 9/11. She served on the Clinton administration's National Security Council staff and as a foreign policy advisor to the Bush 2000 presidential campaign. A Kentucky native, she received an A.B. in East Asian Studies from Harvard University, was a Fulbright Scholar in Hong Kong, and received an M.A. and Ph.D. in political science from Stanford University.