

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

IN THIS ISSUE

Peak China: Personal Observations as a Western Businessperson in China

Patrick Ennis, PhD

Is AI Ready to Help Win Wars?

Lois Hollan and Robert Hummel, PhD

Applying Lessons from the Commercial Innovation System to the National Security Innovation Base

John Wilson

Trusted Access to Microelectronics: Addressing DoD's Unique Issues of Accessibility, Integrity, and Confidentiality of Microelectronics

Ted Glum

AI Technology to Increase US Government Transparency

Rindha Sudhini

ISSUE 9 2024

Robert (Bob) Hummel, PhD
Editor-in-Chief



POTOMAC INSTITUTE PRESS

Copyright © 2024 by Potomac Institute for Policy Studies

STEPS is published by Potomac Institute Press of the Potomac Institute for Policy Studies.

Disclaimers: The Publisher, Institute, and Editors cannot be held responsible for errors or any consequences arising from the use of information contained in this publication; the views and opinions expressed do not necessarily reflect those of the Publisher, Institute, Editors, or any Government Agency. The Potomac Institute is non-partisan and does not take part in partisan political agendas.

Copyright Notice: It is a condition of publication that articles submitted to this magazine have not been published and will not be simultaneously submitted or published elsewhere. By submitting an article, the authors agree that the copyright for their article is transferred to the Potomac Institute Press if and when the article is accepted for publication. The copyright covers the exclusive rights to reproduce and distribute the article, including reprints, photographic reproductions, microfilm, or any other reproductions of similar nature and translations.

Access to this publication is available free online at: www.potomac institute.org/steps.

All images Shutterstock.com, unless otherwise credited.

STEPS (Print) ISSN 2333-3219

STEPS (Online) ISSN 2333-3200

About *STEPS*

STEPS: Science, Technology, and Engineering Policy Studies magazine is the technical publication of the Potomac Institute for Policy Studies, where scholarly articles of broad interest are published for the policy community. We welcome original article submissions including, but not limited to the following:

- Discussions of policies that either promote or impede S&T research
- Articles that address implications and/or consequences of S&T advances on national or international policies and governance
- Articles that introduce or review a topic or topics in science, technology, or engineering, including considerations of potential societal impacts and influences
- Articles that cover historical developments in science, technology, and engineering, or related policies, and lessons learned or implications going forward
- Non-partisan opinion pieces concerning policies relevant to S&T, to include S&T research trends or research opportunities, and the role of national policies to promote or modify those trends and opportunities

STEPS promotes the mission of the Potomac Institute for Policy Studies, which fosters discussions on science and technology and the related policy issues. Policies are necessary to advance scientific research toward achieving a common good, the appropriate use of human and material resources, and significant and favorable impacts on societal needs. At the same time, the creation of effective policy depends on decision makers being well-informed on issues of science, technology, and engineering, including recent advances and current trends.

Societal changes arising from technological advances have often surprised mainstream thinkers—both within technical communities and the general public. *STEPS* encourages articles that introduce bold and innovative ideas in technology development or that discuss policy implications in response to technology developments.

We invite authors to submit original articles for consideration in our widely-distributed publication. Full articles should be between 2,000 and 5,000 words in length, and should include citations and/or references for further reading. Contributions will undergo in-house review and are subject to editorial review. Short articles of less than 2,000 words, such as notes, reviews, or letters are also welcome.

Please submit articles to steps@potomacinstitutione.org

or contact us if you wish to discuss a topic before completing an article. Please refer to the **Instructions for Authors** for complete information before submitting your final manuscript.

Editorial and Production Staff

Editor-in-Chief
Robert (Bob) Hummel, PhD
Email: rhummel@potomacinstitutione.org

Director, Potomac Institute Press
Website + Imaging
Alex Taliesen
Email: ataliesen@potomacinstitutione.org

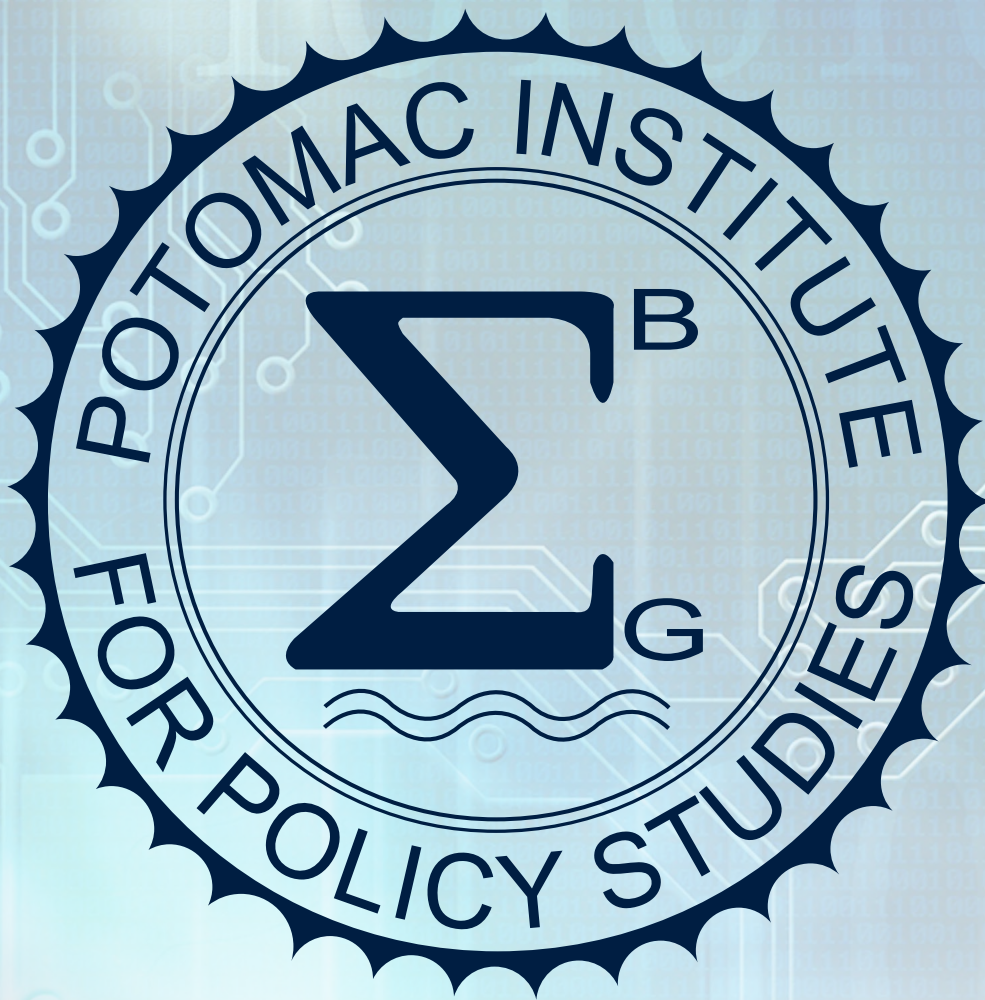
Editing + Design
Sherry Loveless
Email: sloveless@potomacinstitutione.org

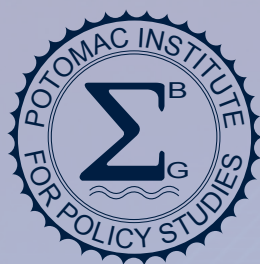
Potomac Institute for Policy Studies Board of Regents

Gen. Alfred M. Gray, USMC (Ret.), Chairman	Hon. Zachary J. Lemnios
Yonah Alexander, PhD	Mark Lewis, PhD
Jeffrey Allen "Skunk" Baxter	Hon. Arthur L. Money
Hon. Maj. Gen. Charles F. Bolden Jr., USMC (Ret.)	Brian J. Morra
Hon. H. Lee Buchanan, PhD	Alden V. Munson Jr.
Peter F. Byrnhrow, PhD	Adm. Robert J. Natter, USN (Ret.)
Terry L. Collins, PhD	Gordon Oehler, PhD
Hon. Rita R. Colwell, PhD	Robie Samanta Roy, PhD
Hon. Matthew P. Donovan	Timothy R. Sample
Peggy Evans	Howard K. Schue
Lt. Gen. Timothy G. Fay, USAF (Ret.)	Hon. Alan R. Shaffer
Raul Fernandez	Brian Shirley
Lt. Gen. George Flynn, USMC (Ret.)	George A. Spix
Melissa Hathaway	Lt. Gen. Keith J. Stalder, USMC (Ret.)
John C. Johnson	Hon. Kathryn D. Sullivan, PhD
Hon. Donald M. Kerr, PhD	Hon. William McClellan
Kathleen Kiernan, PhD	"Mac" Thornberry
Jerry Krassner, PhD	Rand Waltzman, PhD
Francis Landolf	Doug Wolfe
	Lt. Gen. Donald C. Wurster, USAF (Ret.)
	Hon. John J. Young Jr.

About the Potomac Institute for Policy Studies

The Potomac Institute for Policy Studies is an independent, nonpartisan, not-for-profit, science and technology (S&T) policy research institute. The Institute identifies and leads discussions on key S&T and national security issues facing our society, providing an academic forum for the study of related policy issues. Based on data and evidence, we develop meaningful policy recommendations and ensure their implementation at the intersection of business and government.





STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

CONTENTS

About STEPS.	3
About the Potomac Institute for Policy Studies	4
From the CEO	6
<i>Jennifer Buss, PhD</i>	
From the Editor	6
<i>Robert (Bob) Hummel, PhD</i>	
 PEAK CHINA: PERSONAL OBSERVATIONS AS A WESTERN BUSINESSPERSON IN CHINA	 8
<i>Patrick Ennis, PhD</i>	
 IS AI READY TO HELP WIN WARS?.	 17
<i>Lois Hollan and Robert Hummel</i>	
 APPLYING LESSONS FROM THE COMMERCIAL INNOVATION SYSTEM TO THE NATIONAL SECURITY INNOVATION BASE.	 26
<i>John Wilson</i>	
 TRUSTED ACCESS TO MICROELECTRONICS: ADDRESSING DOD'S UNIQUE ISSUES OF ACCESSIBILITY, INTEGRITY, AND CONFIDENTIALITY OF MICROELECTRONICS	 39
<i>Ted Glum</i>	
 AI TECHNOLOGY TO INCREASE US GOVERNMENT TRANSPARENCY . .	 48
<i>Rindha Sudhini</i>	
 Featured Authors	 55

From the CEO

Jennifer Buss, PhD

Publications in the Potomac Institute's journal *STEPS* are where we elevate ongoing discussions of issues of science and technology policy. We continue to see rapid advances in technologies and continuing scientific breakthroughs, both in the US and globally. This environment is challenging US national policies to stay current, relevant, and responsive to the needs for security and economic wellbeing. Articles in *STEPS* are intended to present big ideas to address complex issues impacted by the changing nature of science and technology. These articles are derived from discussions generated by our programs, education, and courses, or from ideas suggested by any of our staff or affiliates. We are a think tank, after all, and *STEPS* is one avenue to document our academic and philosophical debates. We pride ourselves on the diversity of inputs, combining expertise related to the march of science and technology with business acumen and government experience, as brought by visitors, interns, Board of Regents, Senior Fellows, Associates, and others that contribute to the life of the Institute.

I hope you find the ideas expressed in the articles in this issue stimulating and impactful. We welcome feedback and your engagement with the work of the Potomac Institute for Policy Studies.

Jennifer Buss, PhD
Chief Executive Officer, Potomac Institute
jbuss@potomacinstitution.org



From the Editor

Robert (Bob) Hummel, PhD

With this issue of *STEPS*, which stands for Science, Technology, Engineering, and Policy Studies, we present five thoughtful pieces related to US policy considerations that are impacted by advanced science and technology.

Patrick Ennis presents "Peak China," which is his serious proposition that China is entering a long period wherein its capabilities and technology developments will be in descendancy, in contrast to China's history of the past couple decades of phenomenal economic and technological growth. This concept of China's challenges is now repeated often in current geopolitical discussions, but Ennis' theory was presented in a Potomac Institute course on China in March 2023, and the article was made available on the Potomac Institute website in September 2023. Unlike other analyses that are based on economic and demographic data, Ennis' analysis is based on numerous experiences as a businessperson in China and



elsewhere in Asia over the past few decades. His anecdotes buttress facts and figures in a way that can account for human connections and aspirations, and portend a Chinese population that will be increasingly dissatisfied with their lives and prospects. Lest we take heart in their descendancy, Ennis points out that this makes China yet more dangerous at this point in time. There are serious implications for the US in the ongoing trade and technology war with China.

An article by Lois Hollan, for which I am a co-author, is inspired by discussions with Lee Buchanan concerning the use of social media and related digital information sources to provide indications and warnings about intelligence matters. The key idea in those discussions was that the AI breakthrough represented by large language models (LLMs) should provide a mechanism to discriminate between normal situations and unusual circumstances that requires further analysis by intelligence officials. The article advocates for a development project that would leverage LLM technologies in a government and industry program to provide early warning in military and other national security threats.

John Wilson was a major contributor to a Potomac Institute project that produced a report on the national security innovation base, in answer to congressional queries to the Department of Defense on means to support the continued ability of the nation to foster “innovation” in national security spheres. Wilson was particularly concerned with the way in which the innovation ecosystem that has developed (over many decades) in the commercial marketplace to produce start-ups and unicorns and massive business growth—how this ecosystem can be translated to benefit national security interests. Wilson’s article provides some important lessons from the commercial sphere, and some recommendations to the expanding set of initiatives that intend to bring greater innovation to defense systems development and acquisition.

Long before the CHIPS Act and other realizations of the importance of microelectronics to the economy and security of the US, the Potomac Institute was concerned with the strategies for ensuring access to secure microelectronic components for national security. Much of this work was in conjunction with Ted Glum, who was at the time the Director of the US Defense Microelectronics Activity. Now as a member of the Board of Directors, Glum provides a reminder that the CHIPS Act alone does not provide assurance of supplies of secure parts. The misnamed “Trusted Foundry Program” has a long history that Glum outlines. He points out how the program addresses security issues at all points in the production train. As teams across the departments and agencies of the US federal government attempt to ensure that national needs for secure parts can be met, Glum’s article is an important reminder that there are established ways to address security issues according to the needs presented by applications. Glum provides recommendations as to how the program should be enhanced as the nation increasingly “on-shores” factories and facilities that can ensure domestic supplies.

The Potomac Institute hosts interns from US universities, who conduct mini studies during their term in consultation with Institute personnel. Rindha Sudhini, an undergraduate at the University of Pennsylvania, was an intern in the fall of 2023, and her excellent report gave rise to an article by Sudhini in this issue of *STEPS*, concerning ways in which digital record-keeping and information technologies, to include artificial intelligence, can enhance government transparency. At issue is which agencies and elements of the government have the expertise to effect the changes needed that modernize the outmoded and ineffective “freedom of information act” (FOIA) mechanisms. Sudhini makes cogent recommendations.

While enjoying these articles in this issue of *STEPS*, consider contributing an article for subsequent issues. The next issue should focus on challenges and possible solution directions for the next administration, given that the election of 2024 will usher in a new Congress and turnovers at various departments and agencies.

Robert (Bob) Hummel, PhD
Editor-in-Chief, *STEPS*
Chief Scientist, Potomac Institute
rhummel@potomac institute.org


PEAK CHINA

Personal Observations as a Western Businessperson in China

Patrick Ennis, PhD

Senior Partner, Madrona Venture Group and Senior Fellow, Potomac Institute for Policy Studies

Article published online in September 2023 as the white paper: *Peak China: Personal Observations as a Western Businessperson in China*. The Potomac Institute and Editors cannot be held responsible for errors or any consequences arising from the use of information contained in this publication; the views and opinions expressed do not necessarily reflect those of the Potomac Institute, Editors, or any Government Agency.



Many facts, figures, and concurring opinions support the impressions conveyed in this article. Deliberately, data has been omitted to emphasize that these anecdotes and thoughts are not always quantifiable. This can lead to conclusions that might differ from common wisdom. Nonetheless, recent literature contains much data and concurring opinions that corroborate the views of this article. Further reading can be found at the end of the article.

INTRODUCTION

It is fashionable to talk about a “China Rising.” China itself declares its rise, attributing it to a growing economy fueled by manufacturing prowess and increased investments in technological advancements. China boasts of its ascent through statistics, expositions, and Olympics. As a businessperson with years of experience in Asia, including over 50 trips to China, I offer a personal perspective on China’s standing. My view is neither based on official economic data (which is suspect in any case), nor based on China’s propaganda. Instead, I observe that we are currently witnessing “Peak China,” and I believe China will soon start to decline in multiple ways. In my opinion, China is undergoing a process of breaking—and that is not good.

Adversaries tend to be most dangerous when they perceive themselves as weakening. The window of opportunity to win wars is rapidly closing, potentially leading to more belligerent and unpredictable behavior than usual. In our competition with China, if the US can navigate the next several years without a major confrontation with China, the US will emerge victorious. The China of 2030 will be far weaker than the China of 2023. This is a controversial view, as many still believe in China’s growing military and economic strength. My personal observation is that Chinese society is rotting from the inside, and the government is failing politically, beset from all sides. Chinese institutions, including the government, do not have a lot of friends within or outside of China.

The Chinese people, Chinese Americans, and Americans of Chinese descent have nothing to do with the government of China. They did not vote to elect President Xi, and very few individuals truly support him. Criticisms of China as an adversary, whether from the left or the right, target the government or the party, rather than the people. Generalized prejudice against Chinese individuals is counter-productive to US national interests. Indeed, as this article will elucidate, one of the best ways to win against China is to promote increased immigration from China to the United States, especially focusing on attracting young and talented individuals.

CULTURAL IMPACT OF DEMOGRAPHICS

Demographers will tell you that China has a huge problem, resulting from a disastrous 35-year-long one-child program and a historically strong preference for male offspring. However, my observation is that the situation is far worse than the numbers imply.

China has more young single men than women. While the media often quotes the China male-to-female ratio of 105 males to 100 females—this pertains to the total population. Given that women generally live longer than men, the gender imbalance is far greater within the younger age group. This imbalance is evident in practices in society. One egregious example is the importation of young women from countries like North Korea and Vietnam to serve as wives, especially in rural areas. Having a vast population of young men with limited prospects for starting a family is not good. Throughout human history and across the globe, the cohort of young single men often contributes the most to societal turmoil and unproductive behavior.

In China, the society has gotten old before they got rich. This results from a demographic time bomb—an aging society, an incredibly low birth rate, and a per capita income that remains very low. In contrast, other Asian countries, like Singapore, Japan, and Korea, have aging and shrinking populations, but their per capita incomes have already reached world-class standards. In China, except for a few rich cities like Shanghai, Beijing, Shenzhen, and Chengdu, the per capita income in China remains shockingly low. While young people might hope to get rich, the prospects are not great. This reality fosters discouragement. A low-paying factory job does not serve as a good stepping-stone. Fierce competition for slots in top universities persists, yet recent college graduates struggle to find work. The government tries to convince these college graduates to consider factory work. For those students that have the opportunity, pursuing higher education abroad is viewed as a ticket to more opportunities.

It is too late to turn around the birth rate, in China as well as other Asian countries. Efforts to increase birth rates have proven ineffective in countries such as Japan, South Korea, and Singapore, where failed policies included cash payments for children, free daycare, workplace flexibility, and even government-sponsored speed dating. Nothing seems to work and people have seemingly made their choices. In such circumstances, the only alternative to growth is immigration—the lifeblood of a wealth-growth country. Yet, in China, a discussion of immigration is absent. Unlike Korea and Japan, where immigration is increasing despite traditional reputations for being less welcoming of newcomers. China is not very hospitable to immigrants. Immigrants are more inclined to move to places like Singapore, Korea, Japan, Australia, Canada, England, and notably, the United States.

Conversely, the youth—particularly the talented and ambitious youth—in China want to emigrate. One potent strategy to win against China is to increase immigration from China to the United States. Over time, numerous brilliant Chinese scientists and entrepreneurs have come to America to engage in research, education, business ventures, and personal growth. Also on the immigration spectrum, many industrious, hard-working Chinese immigrants have contributed to the United States for generations by aiding in nation-building, raising families, and enriching communities. Welcoming a greater number of Chinese immigrants will weaken President Xi and the Chinese government while strengthening America across the board.

DEFIANCE OF AUTHORITY

The prevailing trend of placing China on a pedestal has often led to the dismissal of voices positing China's upcoming decline. Indeed, China has achieved much, and in some cases, has outperformed the US—for example, in GDP growth rate and in the fielding of certain new weapons systems. This achievement is often attributed to a powerful autocratic government that orchestrates well-planned campaigns. However, my perception is that China's strengths arose despite the autocratic central government and Communist Party—not because of them.

China's innovation and business and cultural vigor have come from the relatively less-regulated entrepreneurial sector that has developed over the past three decades. This vitality is not attributed to government-run, state-owned enterprises. The good things in China are not enabled by the writings of Mao or "Xi Jinping Thought." Instead, they stem from a cultural heritage of social harmony and hard work rooted in thousands of years of family and community focus, underpinned by various religious and philosophical traditions such as Confucianism, Buddhism, and Taoism. However, this vibrancy is independent of the central government. In my view, China is becoming an unhealthy society with a corrupt central government that inevitably paves the way for anarchy and the demise of the ruling system.

President Xi has consolidated power and possesses strength greater than his predecessors. However, many of the local officials and people merely offer superficial agreement while waiting for his tenure to end. The truth is, lawlessness and defiance of central authority is rampant. The military operates with impunity, as evidenced by events like the 2007 satellite explosion that created a space debris field, resulting

in world-wide condemnation and central government embarrassment. I am convinced that similar incidents persist. In the run-up to the 2008 Beijing Olympics, I recall the paid killing and removal of wild dogs from the streets, in defiance of an embarrassed central government that recognized how negatively it was perceived by external cultures. These instances are still discussed to this day. Local governments turn off the required electrostatic scrubbers on coal power plants to enhance efficiency, only activating them for a day when the Beijing inspectors visit. President Xi attempts to consolidate power that he has not yet achieved.

A long-standing policy requires foreign businesses in China to employ a senior member of the Communist Party, which deters international investors. In one of my companies' office in Beijing, we had to create a position for someone who nominally reported to the CEO of our China entity. The government in Beijing filled the position, assigning an older gentleman who had been educated in the United States. Although we knew he was always reporting back to the government, I believe he had mixed allegiances—it was not clear whose side he was on. Many of the ruling elite in China have children who have settled abroad in wealthy countries. The government may think that their central control is benefitting China, but it has led to a cadre of people with split loyalties and freelance operations.

China is frequently accused of propelling their rise by stealing US intellectual property. Many documented cases of this theft exist, especially from the 1990s.

Many Chinese companies are based upon Western ideas, and some on stolen intellectual property. During one of my trips to Shanghai about 10 years ago, I was at a government research institution meeting with several top R&D people to discuss potential collaborations. In one session, a series of professors were proudly presenting their reverse compiler work. There was no sense of shame and no ambiguity that the whole purpose of this work was to steal source code from other developers. They knew this was illegal and indefensible but assumed it was socially acceptable to be in open violation of laws and rules.

In other cases, they steal from one another. When establishing our Beijing office and hiring about 15 individuals, our local advisors informed me to expect that everyone in my group would have one or more additional employers (potentially competitors). In the relevant field in the US, this would be unallowed, and I had to ensure that our staff were not

overtly stealing information to share with other employers. Their motivation likely stemmed from a desire to earn extra money, but there was little impunity or effort to conceal this secondary employment. While from my Western cultural perspective, theft is morally wrong, the culture accepted some amount of theft as the way to succeed.

Some companies have succeeded. Seeded by global technology innovations, some Chinese companies have become international competitors. However, the notion that somehow the Chinese government is responsible for China's world-class companies is a misconception. In reality, companies like Lenovo, Huawei, ZTE, Tencent, and others, arose expressly because the Chinese government intentionally took a hands-off approach. These companies thrived under a capitalist framework, while it lasted. In contrast, typically state-owned enterprises neither operate on an international level nor engage in significant exports.

WHO IS CHINESE?

China is a far-flung, diverse country with a population of more than 1.3 billion. Ethnically, Han Chinese make up approximately 70% of the population, according to official records. However, numerous other ethnic groups and mixed ethnicities contribute to the diversity. The term "Han" is a default category encompassing many subgroups, rendering it too broad to be meaningful. The term is similar to saying someone in Portugal is the same as someone in Switzerland because they are both "European." Despite this, the Communist Party tries to promulgate a perception of uniformity among Han Chinese, and by extension, the entire population of China. For the increasing portion of the population not categorized as Han Chinese, their position in one or more ethnic underclasses leads to them feeling marginalized and discriminated against. China exhibits this distinctive characteristic in contrast to countries like Japan or Korea, which are closer to true monocultures. Yet, China's government tries to run China as a monoculture, championing the "China way." This practice of pretending a country is a monoculture when it is not is destabilizing. Diverse countries can be challenging to govern, but they are impossible to govern if the diversity is not acknowledged.

The central government in Beijing is not as powerful as commonly believed. The local governments retain substantial power, and many people simply ignore the government rules. Society is based on who you know and who you can bribe. I have not seen the equivalent in modern Japan or

Korea, for example. Xi has forcefully attempted to exert the primacy of central control over the provinces and cities, but a natural tendency in China is to resist control.

PHYSICAL AND CULTURAL ROT

Behind the glittering façade of the fancy buildings and upscale hotels lies a story of shoddy workmanship and pervasive corruption. Take, for example, two exclusive high-end business hotels in Beijing, where I frequently stayed after their openings in 2007. When they first opened, these hotels looked amazing, yet after a couple of years, the hotels were literally falling apart. The glass roofs were leaking because the panes were installed improperly. Bathrooms were malfunctioning because the plumbing contractors omitted p-traps to save time and money. Tilework was disintegrating after a few years. According to my Chinese friends, even the most high-profile architectural projects involve shortcuts by corrupt construction companies.

Equally astounding is the sight of countless empty modern high-rise condominiums—a glaring misallocation of capital. These structures hold little to no value, like worthless stock, given their low quality and redundancy in light of China's shrinking population and hostility to immigration.

Wasted investment can be a form of corruption. China has been successful in developing technical expertise in certain areas; however, its efforts in advanced semiconductor production have fallen flat. Over 20 years ago, I visited China on behalf of a Seattle semiconductor startup. Our search for fabs to manufacture our chips led us to deep discussions with various Asian chip manufacturers. In China, Grace Semiconductor and SMIC, whose capabilities were inferior at the time, spoke of the billions of dollars of government investments that would soon elevate them to world-class status. Yet, 20 years and the equivalent of many billions of dollars later, China remains far from attaining the capabilities of TSMC, Samsung, or Intel. It takes more than just financial infusion to achieve excellence in a field.

Corruption further taints business deals. Business everywhere is based on relationships to impress partners, but in social settings involving business counterparts, I have observed open behavior that I have not seen in other countries.

At dinners with senior business executives and government officials, these older male executives were accompanied by younger female companions who were literally introduced as their "second wives." Some executives even boasted of

having third wives. In China, if you are a senior government official or businessman, having a second wife is exceedingly common. You would in fact stand out if you didn't have a regular companion to bring to the business dinners and karaoke evenings. The unabashed disregard for the law in China speaks to a state of official business and government culture that undermines trust and defeats sound international business practices.

CHINA'S DEPENDENCIES

The US enjoys abundant natural resources, including energy supplies, food production, and mineral deposits. In contrast, China faces problems in certain areas. China relies on massive energy imports for power. While they have ample coal reserves and a nuclear program, China remains a significant importer of fossil fuels. China also struggles to feed and hydrate its population.

At the same time, China exports some of its best human resources and investment capital—a phenomenon known as brain drain. This trend has been ongoing for decades and has recently accelerated. Various centers, such as Vancouver, New York City, San Francisco, Seattle, Sydney, and Singapore have welcomed Chinese immigrants. In recent years, significantly higher numbers of Hong Kong Chinese have relocated to Singapore due to China's unilateral abrogation of the Sino-British Joint Declaration, which promises "one country—two systems." Each of these centers provides a cultural environment conducive to Chinese relocation outside of China. For example, Singapore citizens are predominantly ethnically Chinese from southern China—with many having been in Singapore for two or more generations. Consequently, these individuals feel little affinity towards China as a government, while retaining a strong connection to Chinese culture and people, including aspects like food, literature, and religion.



During my trip back to Singapore last year, which marked my first return since the COVID lockdown, I learned that the influx of people from Hong Kong to Singapore had been so significant that it sparked the development of anti-China sentiment. I observed this judgement in Singapore for the first time in my 20+ years of visiting the country. The derogatory comment heard originated from a third-generation Singaporean of high social class, who viewed Hong Kong immigrants as less desirable individuals despite their wealth and education. This phenomenon underscores the massive emigration from China.

Additionally, there is a money drain. China's much touted Belt and Road initiative is floundering. Many of the projects constructed by China were poorly executed and are deteriorating after just a few years (much like my luxury hotel experience mentioned earlier). Foreign countries may accept the Chinese money and projects, but they do not envy, respect, or trust the Chinese government. The Chinese government dispatches their own workers who treat local residents as inferior and incapable of handling complex endeavors. This approach does not engender goodwill, and the potential return on investment for these projects remains uncertain.

Even private investors spend as much money abroad as possible due to their lack of confidence in prospects within China. If sufficiently affluent, they acquire second homes in the United States, Australia, Singapore, England, or elsewhere. They also prefer sending their children to schools in the United States or abroad. Furthermore, they distrust the cleanliness of their food, water, and air. What does this signal for a country that aspires to become the world's most powerful? It just does not add up.

Chinese banks are generally unhealthy, as the debt burdens carried by Chinese entities are far worse than in the United States. The focus on real estate as the main source of savings and wealth creation poses a big problem for China.

LET THEM STAY

When I started graduate school in 1985, the entering PhD class in physics at Yale consisted of 20 students, including 6 American citizens and 2 students from mainland China. I became acquainted with those two students, both of whom were among the brightest students in China, earning them the opportunity to study in America. They are both now long-time US citizens, enjoying productive careers on Wall Street, in management consulting, and as startup founders.

Today, graduate schools are filled with Asian students, with many from mainland China. Numerous factors drive Asians to American schools; with some Chinese students citing the reasons I have discussed. But another powerful reason is the limitations of the Chinese educational system, which focuses heavily on tests, rote learning, and deference to professors as authority figures.

In my own experience within a graduate program, recent Asian immigrants routinely outperformed Americans on placement tests and classwork exams. However, over the course of the multiyear program, Americans (and immigrants who studied in America as undergraduates) usually produced more creative and influential research. Today, graduates of American doctoral programs are more likely to publish their original creative work, rather than solely implementing the plans of a thesis advisor.

While certain Chinese universities have attained world-class status, prospective students in China are aware of the prestige and creative research training at US institutions. Consequently, they flock to US educational programs if given the chance, or at least attend schools outside of China when possible. Students that come to the US generally want to stay in the US after graduation. Perhaps this is a testament to the breadth of topics covered in the American education system, where students are taught to ask "why" and to question their professors and academic dogma. These are attributes that I believe lead to more creative and productive technologists.

WHAT IS NEXT?

While many supporting facts and statistics exist, quantifying many of my anecdotes proves challenging. No single factor alone points to China's demise, but my overall impression is that we have witnessed "Peak China." This does not mean that China will cease to pose problems for the US in military, economic, or political affairs. Indeed, the challenges could intensify as the government in China increasingly and desperately clings to the illusion of China's continued rise. President Xi, who has become increasingly autocratic, already points to this phenomenon. His legitimacy depends upon perpetuating the charade and convincing the Chinese populace that their nation will soon emerge as the strongest, richest, and most respected in the world.

After the Tiananmen Square massacre, I attended a lecture by one of their top student leaders, who had escaped to

America. She spoke optimistically, saying that China would change because the youth yearned for democracy. For decades, I shared her optimism as China seemed to be transforming into a freer society both economically and culturally. However, President Xi has turned back the clock, reversing this progress. Recently, I spoke with a young Chinese colleague working in the US and about to obtain a green card. This colleague's sentiments mirrored those of the student leader 33 years ago—that the arc of history is against President Xi because the youth want democracy. Why would it be any different this time? While young people may feel change is inevitable, history suggests otherwise.

I fear that without a change in regime, President Xi and his party will cling to power, preventing a peaceful, smooth transition to democracy and free markets. Moreover, a new regime may be as bad as the old. Thus, the apparent opportunity lies in welcoming talented young individuals to the United States, where they can become citizens and start businesses. However, this leaves over a billion Chinese lacking the means to emigrate in a precarious situation. This situation affects not only the United States and the free world, but also China, itself. The US and Chinese economies are intertwined, with continued cultural mixing. China possesses modern military technology. Alongside our allies such as South Korea, Japan, and Taiwan, we should fear not only an ascendant China, but rather a collapsing China.

ACKNOWLEDGEMENT

I thank Dr. Robert Hummel, Chief Scientist of the Potomac Institute, for his expert energetic assistance with this article.

FURTHER READING

Adam S. Posen. "The End of China's Economic Miracle, How Beijing's Struggles could be an Opportunity for Washington," *Foreign Affairs*, Aug 2, 2023.

Sandan and Dhume. "China Can't Seem to Make Friends or Influence People," *Wall Street Journal*, Opinion. Aug 3, 2023, <https://www.wsj.com/articles/china-cant-seem-to-make-friends-or-influence-people-popularity-beijing-economic-rise-asia-polls-2779690b>, and Aug 4 print edition.

Michael Bluhm, "End of an Age," *The SIGNAL*, Sept 29, 2022, Subtitle: "What's wrong with China's economy? Jeremy Mark on the property crisis, income inequality, and the need for a new economic model." <https://www.thesgnl.com/2022/09/china-economy-challenges/>.

The Economist, "How much trouble is China's economy in?" "Growth is faltering and country is flirting with deflation," July 17, 2023, <https://www.economist.com/finance-and-economics/2023/07/17/how-much-trouble-is-chinas-economy-in>, Print edition "Feel-bad recovery" July 22, 2023

Bloomberg News. "China's Economic Woes are Multiplying – And Xi Jinping Has No Easy Fix," June 29, 2023, updated June 30, 2023, Subtitle: "China is facing a confluence of problems: Sluggish consumer spending, a crisis-ridden property market, flagging exports, record youth unemployment and towering local government debt." Paywall: <https://www.bloomberg.com/news/features/2023-06-29/china-economic-rebound-falters-weighed-by-debt-property-slump-little-stimulus>







Is AI Ready to Help Win Wars?

Lois Hollan, Senior Fellow, Potomac Institute for Policy Studies

Robert Hummel, Chief Scientist, Potomac Institute for Policy Studies

INTRODUCTION

Artificial intelligence (AI) is expected to transform the way wars are fought and revolutionize the enterprise of national security. However, it is still unclear how this technology can be successfully leveraged for national security purposes. The problem stems from the ambiguity of the term “intelligence.” Intelligence is generally taken to mean: “the ability to learn or understand or to deal with new or trying situations: reason; also the skilled use of reason.”¹ But current AI systems are “artificial” and neither perform reasoning beyond their training nor adapt to novel situations. The value of AI to national security will be in accessing data to provide relevant, confident, and reliable information to operators, analysts, and commanders in a real and uncertain world. In this article, we examine the kinds of data that AI technology might address, the challenges of exploiting that data, an approach by which AI could enable a new dimension in the recognition of threats, and why we should develop those capabilities now.

Automation technologies are already supplanting human analysis of vast amounts of sensor data to understand “the battlespace.” Techniques have been developed to perform “automated (sometimes assisted) target recognition” (ATR) to identify tanks, other military ground vehicles, aircraft, ships, submarines, and objects of significance to military operations. Exquisite sensor systems have been developed to collect data to feed into recognition systems. Such sensor data supply both human and machine recognition systems, with the latter employing both classical and emerging AI techniques to recognize threats.

Yet, these elaborate systems have failed to adapt to two new realities:

1. A massive amount of timely data is available for public consumption, which is considered unconventional and separate from the capabilities of exquisite sensor systems designed to collect (conventional) battlespace information; and
2. The kinds of items, threats, and events that must be recognized are distinctly different from the artifacts of war that have been modeled and taught to existing recognition systems.

Related to (1), there is a great deal of accessible digital data (such as social media, cell phone data with images or videos, Twitter [now X] content, news commentaries, and search engine queries). These timelier sources dominate traditional intelligence-gathering sources.

Regarding (2), it is important to recognize that the battlespace is increasingly shaped by influence operations, psychological techniques, civilian technologies, and economic and political dynamics. These novel operations elude current recognition systems; can be engaged before, during, and after kinetic conflict; and can replace kinetic warfare. Recognizing propaganda, deep fakes, nefarious ideological intent, and foreign influence has become as important as tracking troop movements or detecting tank convoys.

So maybe we’ve been doing it wrong or, at least, not keeping up with the times. AI may be the panacea, but likely not in the way that we have been expecting.

ACCESSIBLE DIGITAL INFORMATION

Accessible digital information comes in many forms (see Figure 1), is often unstructured, and requires interpretation. It becomes clear that the use of accessible digital information—including social media—changes the nature of military intelligence, information gathering for national security, and even the role of the “warfighter.”

The explosion of available digital information has vastly multiplied the opportunities for and scope of exploitation capabilities. This is especially true for commercial and public sector applications. The US government, however, has only begun to leverage such opportunities for national security and automated exploitation purposes.

The Challenge of Exploiting Accessible Digital Information

Exploitation of open-source digital information has been used in various high-profile criminal and military cases. Often, data comes from video cameras used for surveillance by local businesses or individuals. Still images and videos are also volunteered by individuals using smart phones as cameras. In the Boston Marathon bombing of April 15, 2013, imagery from over 13,000 videos were exploited by professional and crowd sourcing analysts.² The massive amount of available video and other data led to a realization of the importance of volunteered, popular footage.

Since then, the government has accelerated efforts to use multimedia data to maximum advantage. The FBI has established the **Multimedia Exploitation Unit**, which employs advanced video processing technology³ (called the MXU) to use multimedia data for identifying leads in criminal cases. The US Department of Homeland Security (DHS) has established a program called **War Crimes Hunter** to deny

US entry to persons engaged in war crimes and human rights violations. The program collects data from the Human Rights Violators and War Crimes Unit within DHS's Homeland Securities Investigations, and collects online imagery and evidence to publish facial images and other biometric data of perpetrators.⁴ The New York Police Department's **Domain Awareness System** (DAS)⁵ collects data from cameras and sensors throughout the city to forensically solve crimes. Its work is controversial due to implications of invasion of public

privacy.⁶ Recently, it has been reported that DAS will integrate the use of Ring surveillance cameras.⁷ National fusion centers were established after 9/11 to receive both classified and unclassified data from governmental and open sources, and to share information with state and local government agencies.⁸ There are 80 such fusion centers throughout the United States that can provide counterterrorism support to the federal government. Similar to the DAS, their use is also controversial.⁹

Figure 1. Digital Information Sources

Below is a proposed categorization of what we might consider "accessible digital information:"

Owner-disclosed Open-Source Data: Freely volunteered open-source data is any information that is posted, published, or disseminated and is available to anyone for any reason, free of charge. This type of information is typically available to anyone with an Internet connection. The value of exploiting owner-disclosed open-source data lies in its unrestricted usage. However, the veracity of the information can be suspect, and it can be difficult to align with specific applications.

Volunteered Information: Sometimes individuals voluntarily give authorities information that is not publicly available. Such "tips" are received by law enforcement as well as intelligence authorities and news outlets. Individuals with security clearances have a duty to report observations and suspicions. Examples of volunteered information include identifying insider threats or adversarial spies.

Accessible Open-source Data: Information that can be purchased includes newspaper publications and materials available through paid subscriptions or newsstand purchases, and online content behind paywalls. The purchaser is the intended recipient of the content. The intelligence community uses the term "publicly available information" (PAI) to include anything that is available to the public but may be copyrighted, require payment for access, and be subject to end-use agreements. Government use of such information is subject to restrictions.¹⁰ Commercial satellite data fall into this category.

Profiling Information: Online resources use account information or "cookies" to track individuals' activities within and across computer applications, thereby collecting information about them. By clustering information across various dimensions, individuals can be profiled according to their attributes. This information is exchanged and sold, especially to advertisers, political campaigns, and brokers who use it for profit and gain.

National Technical Means Sources: Systems procured by government agencies for government collection of information, for example through the use of satellites, are continually upgraded and improved to provide classified information about activities on Earth.

Purloined Information: Government intelligence services engage in the business of pilfering secrets from foreign entities. When the information is not intended to be shared but has been obtained through nefarious means—which can include illegal hacking or espionage—then the information has been purloined.

In 2005, based on recommendations of the 9/11 Commission and the Robb-Silverman Commission to counter weapons of mass destruction,¹¹ the US established a branch of the Office of the Director of National Intelligence (ODNI) called the Open-Source Center for exploiting information of overseas activities. The Center succeeded the Foreign Broadcast Information Service (FBIS), which had focused on intercepted foreign language messages and publications. Congress had long recommended that the intelligence community (IC) make greater use of open sources, but codified these recommendations in the “Intelligence Reform Act” of 2004.¹² Today, the renamed Open Source Enterprise (OSE) is part of the CIA’s Directorate of Digital Information (DDI). However, there are continuing concerns that open-source intelligence is underutilized.¹³

The OSE gleans open-source data from newspapers, internet postings, publications, and other sources, which are collectively labeled open-source intelligence (OSINT). When combined with classified sources (e.g., SIGINT or IMINT) it is “all-source intelligence,” which can be exploited by other elements of the IC. Like all intelligence activities, the output may be useful for military operations, but is generally aimed at national decision-making activities.

An example of OSINT is the geolocation of adversarial activity that can be acquired from posted imagery such as selfies and terrorist recruitment videos. DARPA and IARPA co-sponsored the development of a software system using a semi-automated process to geolocate imagery for which the metadata have been stripped (as is customary for posted imagery).¹⁴ The techniques have been adopted by news organizations and private companies to assist analyses such as forensic analysis of war crimes in Ukraine.

Within the US IC, the Defense Intelligence Agency (DIA) leads the National Media Exploitation Center (NMEC), which recently has been refocused on analysis of Chinese military actions. The DIA practices all-source intelligence analysis to understand installation and movements of foreign military assets and their capabilities, including exploitation of OSINT and social media.

The Dutch firm Bellingcat is famous for using open-source information for its forensic investigation of Russian involvement in the downing of flight MH17 in July 2014.¹⁵ Bellingcat has continued to leverage open-source information in ongoing investigations of atrocities in Ukraine. Because their independent findings are not classified, intelligence agencies can openly discuss their work.

The Ukrainian company Molnar performs open-source investigations, publishing findings in English, in support of Ukraine's defense against Russia.¹⁶ For example, Molnar identified a missile factory near Moscow as a source of weapons being used against Ukraine.¹⁷

The Challenge of Too Much Data

Such examples demonstrate the power of exploiting accessible digital information. At present, however, there is relatively little automation beyond the formatting and dissemination phases of data processing. Much of the analysis is performed by human analysts who are inundated by the sheer volume of available data. Analysts must comb, interpret, correlate, and productize data from multiple sources, often operating within a compressed operational timeframe.

These techniques are labor intensive and require specialized analysts trained in image processing methods, text filtering, and object recognition software. Still, it is human analysis that generates useful intelligence derived from multiple sources.

Decades ago, researchers bemoaned the “pixels to pupils” ratio, wherein the number of pixels that had to be analyzed far exceeded the capacity of the number of human pupils available to attend to those images. Thus, many images

and pixels were left unobserved. Today, the situation is far worse. In addition to imagery deliberately collected by specialized sensor systems, all media in accessible digital data—combined with commercial and national collection systems—confront yet fewer analysts. Thus, the challenge is to choose which data to view and analyze.

Moreover, there is only incipient use of novel data types. Despite concerns over US civil liberties and individual privacy, new data sources can provide greater security by affording defensive and intelligence-gathering measures without impinging civil rights. The fact that adversaries are using these sources and technologies against the United States only emphasizes the urgency to recognize and defend against nontraditional combat operations using all available sources of information. Simply, valuable data cannot remain unobserved and unused.

Many hope that we can supplement the number of analysts by making use of AI to create virtual analysts. But AI is not truly “intelligent” in ways that human intelligence reasons about threats. If AI is to be used, it will not be to reason about data, but rather to assist human analysts extract relevant data from large volumes of incoming data.



The Challenge of Over-specification

Current approaches to analyzing data (whether government sensor data or other accessible digital data) largely focus on finding specific targets that are known and/or well characterized. Targets might be military vehicles, missiles, radar sets, or other well-defined objects that present specific signatures. In more complex situations, recognition of events or intentions relies on detecting specific indicators in sufficient numbers; but those indicators, in turn, rely on recognition of well-specified objects or activities. Automating the process of recognition (e.g., automatic target recognition) accelerates the search for indicators.

Regardless of how precisely an object is characterized, it remains that increasing amounts of data can lead to false alarms. False alarms must be recognized and negated by human analysis, especially given that false positives can lead to adverse consequences. The propensity for excessive false alarms renders automated recognition systems worthless.

Further, recognition techniques based on detailed modeling fail to account for new types of targets. Rarely do techniques use context and higher-level reasoning that are implicit to human thinking. Machine-learning approaches attempt to overcome this impediment but can lead to overtraining and a narrowed understanding of targets. Such systems often fail in real-world, evolving, and unknown situations. Thus, a different approach is needed to enable exploitation of massive amounts of available data.

A NEW DIMENSION IN AUTOMATED RECOGNITION OF THREATS

A viable solution involves discerning between mundane data, normal data, and data that need careful attention. This requires a more abstract view of the world. The questions is not “What kind of tank is this?” but rather, “Is this a normal event or scene?” If we can focus analysts’ attention on locations and events that require attention, we can liberate the time and effort required to check on normal situations.

The central construct is to perform automated screening of data to filter out normality and to detect anomalous situations that require further analysis. Instead of trying to detect precisely modeled objects, automation should present human analysts with small and highly relevant portions of data that can assist in their assessment and understanding of the situation. By discarding the mundane, we vastly

increase the breadth of data that is effectively processed. The data that should be discerned for normal versus abnormal situations entails the joint use of imagery, text, audio, and all accessible digital information.

The technical challenge is to define normality for the system to properly filter the data. Normality is a statistical phenomenon, and in multimedia environments of different data sources, it is defined by complex and highly interrelated multivariate distributions. Recent advances in AI have demonstrated an ability to parameterize complex multimodal distributions. At issue is whether such models can sufficiently characterize normality to automate sifting and analysis of accessible digital information.

Large Language Models

The technology of large language models (LLMs) represents a breakthrough in AI, which has demonstrated that generative techniques can create realistic text and images. Evidence shows that the statistics of normal text and images can be encoded in a “model” with a (mere) few billion parameters¹⁸ within the framework of a graphical network. The statistics can be modeled so accurately that generative methods are able to produce text and images that appear normal (as opposed to nonsensical noise).

Since normality can be effectively modeled, it should be possible to detect what is “not normal.” Statistical parameters of normality might need to be dependent on location, or categorization of location type. For example, these systems could model normal activity in an urban environment or normal tweets in the Middle East. Developing a model of normality, from all kinds of accessible digital data will likely require careful curation of data, so as not to pollute the model with unusual occurrences (that perhaps should draw attention). The development of a model that parameterizes “normality” should be based on multiple data sources so that dependencies and correlations can be modeled across multiple dimensions of features.

Moreover, it may be necessary to train systems to recognize the kinds of “not normal” circumstances that are of interest. Because these are (presumably) rare events, it will be useful to simulate patterns that should be flagged by a recognition system. Of course, simulations will use generative models trained in an adversarial fashion, which then may be used to bootstrap a recognition system capable of detecting targeted anomalous activities. Such simulations

would involve multiple modalities to mimic an abnormal situation that warrants attention.

Therefore, it is not the precise “form of a tank” in an urban setting that is a cause for concern, but rather the movements of a set of tanks through a downtown area where tanks are not normally present. A screening tool should detect such unusual circumstances by combining images, texts, “tweets,” search engine queries, and metadata about the locale and environment at large. Available digital information will presage concerns by locals that can be indicative of early stages of conflict or disasters. The mix of different information sources provides confirmation of abnormal conditions.

A RACE FOR INTELLIGENCE

The technology of LLMs has rapidly developed over the past decade, yet to date has been limited in application to generative models. Those models have now become commercially available, if not fully monetized. This is an opportune time to explore the use of technologies of complex models to screen for abnormality in available digital data to be employed for national security purposes.

We propose a program that would develop techniques to screen all forms of digital information for anomalous patterns that might be of interest to analysts. The system would sift massive amounts of available data, in real time, to find unusual patterns that can provide warning of military plans or activity. This information would be filtered by geographic regions of interest and used to alert teams of expert analysts about significant findings.

The process of building models for national security purposes will be labor and cost expensive. The number of “tokens” that must be extracted as “features” in the data will be large when compared to today’s LLMs. Processing training data will necessitate considerable computer resources. Curation of training data will need to ensure that the corpus of data to be searched is relevant to each domain chosen for modeling. The generation of target scenarios will require complex scripts and production.

If successful, such an alerting system, built on large language modeling technology, would provide a powerful cutting-edge capability for national security by providing early warning and attributional evidence for adversarial activity. The first to acquire this capability will have a major global intelligence and defense advantage, which will enable

countering disruption and/or aggression before it becomes critical. **The LLM breakthrough that gave rise to surprisingly good generative models would now be leveraged for important defense capabilities.**

The technology and computational power exist to build a system that ingests streams of accessible digital data, correlates these data with normality as modeled by the system, examines anomalous patterns to recognize the kinds of non-normal situations that should be flagged, and rapidly brings relevant data to the attention of analysts who can easily corroborate or deny the concern.

While this challenge is not easy, the technological advances in AI and LLMs point to viable solutions. The United States currently has an advantage over other nations’ development and experience with AI information technologies. But there is no guarantee that the development of such a screening system will happen first in the US. The race to develop systems that leverage new sources of accessible digital data and screen for relevant defense and intelligence information has already begun.

SUMMARY

A principal hope for enterprises in AI is to develop capability to manage and discover intelligence from massive amounts of available data. The intent is that AI systems will supplant much of the human labor currently needed to cull data and replace current methods that can only access a fraction of the available data. With the ever-expanding availability of data (particularly open-source data), the need for such AI tools is rapidly increasing.

In the past, AI techniques have been used to assist in tracking objects; identifying vehicle types; correlating “tweets” and other online postings with events and geolocation; and alerting of changes in scenes. These techniques have very specific applications and provide utility, but fall short of accommodating the deluge of multiple dependent data sources or novel data types. Furthermore, these techniques neither address nor consider the changing nature of threats.

It should be possible to train an AI system to recognize anomalies of military significance. LLMs have surprised the technology world with their ability use billions of parameters in deep networks to model complex statistical patterns of language and imagery, when provided sufficient training examples. The generative aspects of existing models (e.g.,

in ChatGPT®) demonstrate the ability to model normality and might be useful for generating examples of anomalous activities that need to be recognized in text and imagery.

Training and development processes require access to massive amounts of prior data—groupings of data that have been labeled according to whether the instance is “normal” or “relevant,” wherein “relevant” might be “of military significance,” or might (in other applications) be categorized by other criteria. The key is that recognition of events must be broad-based, as opposed to specifically focused on a set of target vehicles, patterns, images, and/or words.

The proposed research program would require full participation of and collaboration with the US government to access requisite training data and effectively guide the development process. It will be crucial to train systems with curated data sets that intentionally either include or do not include unusual military activity.

Importantly, the system is not requesting that an AI system do any reasoning or apply actual intelligence to the analysis of situations. Instead, the program would apply techniques that have demonstrated value, namely, the ability to model statistical patterns that result in “nothing significant to report.” It is the parameterization of statistics that can differentiate between “normal” and “not normal” activities that leverage breakthroughs in AI for the benefit of national security.

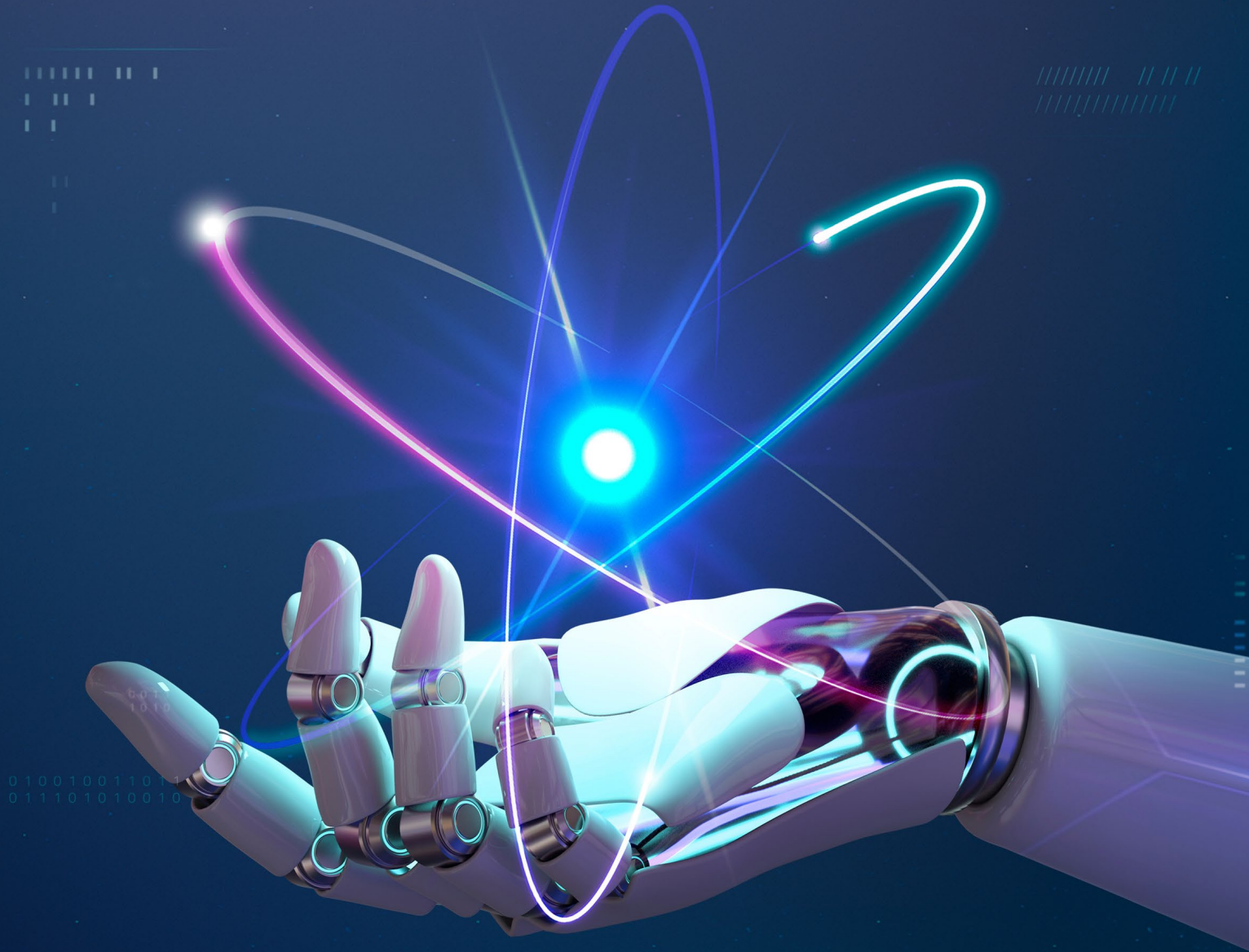
ACKNOWLEDGEMENTS

The authors are grateful for discussions with the Honorable H. Lee Buchanan, whose ideas on the use of social media and LLMs directly led to this paper.

ENDNOTES

- 1 “intelligence,” in Merriam Webster, 2024
- 2 Johnny Nhan, Laura Huey, Ryan Broll, “Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings,” published Dec, 2015, in *The British Journal of Criminology*, Volume 57, Issue 2, 1 March 2017, Pages 341–361, <https://doi.org/10.1093/bjc/azv118>.
- 3 Thomas Brewster, “This Secret \$35 Million FBI Unit Mixes Facial Recognition With Big Data To Investigate America’s Most Horrific Crimes,” *Forbes Magazine*, July 2020, This Secret \$35 Million FBI Unit Mixes Facial Recognition With Big Data To Investigate America’s Most Horrific Crimes (forbes.com)
- 4 Alyssa Erichs, *Privacy Impact Assessment for the War Crimes Hunter*, Department of Homeland Security, 28 May 2020, https://www.dhs.gov/sites/default/files/2022-03/privacy-pia-ice056-warcrimeshunterappendixupdate-march2022_0.pdf

- 5 E.S. Levine, et al., “The New York City Police Department’s Domain Awareness System”, *Informational Journal on Applied Analytics*, Volume 47(1), 18 January 2017, Pages 70-84, <https://pubsonline.informs.org/doi/10.1287/inte.2016.0860>
- 6 Ayyan Zubiar, *Domain Awareness System*, Surveillance Technology Oversight Project, 26 September 2019, Domain Awareness System – S.T.O.P. - The Surveillance Technology Oversight Project (stopspying.org)
- 7 Daniel Schwarz, et al., *The NYPD is Teaming Up with Amazon Ring. New Yorkers Should be Worried*, NYCLU, 11 January 2023 <https://www.nyclu.org/en/news/nypd-teaming-amazon-ring-new-yorkers-should-be-worried>
- 8 Department of Homeland Security, *National Network of Fusion Centers Fact Sheet*, 09 January 2023, <https://www.dhs.gov/national-network-fusion-centers-fact-sheet>
- 9 Michael German et al., *Ending Fusion Center Abuses*, Brennan Center for Justice, 15 December 2022, <https://www.brennancenter.org/our-work/policy-solutions/ending-fusion-center-abuses>
- 10 The Civil Liberties and Privacy Office, *Civil Liberties and Privacy Guidance for Intelligence Community Professionals*, Office of the Director of National Intelligence, July 2011, https://www.dni.gov/files/documents/CLPO/CLPO%20Publication_Publicly%20Available%20Information_July%202011%20-%20Public%20Release%20Version.pdf
- 11 National Commission on Terrorist Attacks upon the United States, Thomas H. Kean and Lee Hamilton, “The 9/11 Commission Report,” 2004; Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction”. United States Department of State. Washington, D.C.: Federal Government of the United States. February 6, 2004
- 12 *The Intelligence Reform and Terrorism Prevention Act of 2004*, Civil Liberties Privacy Office, Office of the Director of National Intelligence, December 2004, <https://www.dni.gov/index.php/ic-legal-reference-book/intelligence-reform-and-terrorism-prevention-act-of-2004>
- 13 Chris Rasmussen, *Avoiding the Secrecy Trap in Open Source Intelligence*, The Cipher Brief, 21 March 2023, *Avoiding the Secrecy Trap in Open Source Intelligence* (thecipherbrief.com)
- 14 *Intelligence Advanced Research Projects Activity, Finder*, Office of the Director of National Intelligence, IARPA - Finder
- 15 *MH17: The Open Source Evidence, A Bellingcat Investigation*, <https://www.bellingcat.com/app/uploads/2015/10/MH17-The-Open-Source-Evidence-EN.pdf>
- 16 *Molfar*, Molfar Limited, <https://molfar.com/en>
- 17 *Kh101, Kh555, Kh69: Where does Russia make its missiles?*, Molfar Limited, <https://molfar.com/en/blog/fabryka-raketnogo-teroru-de-i-yak-rosiyany-buduyut-rakety-yakymy-obstrilyuyut-ukrainu>
- 18 However, GPT-4 is said to have more than a trillion parameters; see <https://the-decoder.com/gpt-4-has-a-trillion-parameters/>



Applying Lessons from the Commercial Innovation System to the National Security Innovation Base

John Wilson

Senior Fellow, Potomac Institute for Policy Studies





INTRODUCTION

Over the past few decades, an ecosystem of companies and structures has emerged that encourages and supports innovations and their transition into viable products. Venture capital (VC) markets and VC firms are prime examples of such support structures. These and other structures first developed in the commercial marketplace, which we might call the “commercial innovation system.” Similar structures are increasingly being adopted, sometimes in different forms, in government and national security environments.

Recent policy discussions of the US Department of Defense and congressional oversight committees have used the term “National Security Innovation Base” (the NSIB) to describe those elements that support national goals. These elements can be categorized, and best practices from the commercial system can be applied to foster innovation in national defense. Inevitably, however, we must confront the complex notion of “innovation” given current components and participants, and

how innovation in the traditional commercial sector is being transformed for applications across the NSIB.

An overarching issue in support of innovation is the attribute of *time*, as required for the development of an idea, to change course, and overall time to market. Commercial technology markets have developed platforms and methods that accelerate the time scale to rapidly grow startups into unicorns to lead the contemporary world’s largest and most advanced economy. Speed is a primary goal of commercial innovation systems in all aspects of development.

The issue is how to develop analogous platforms in the national security sector that can bring similar value to the NSIB and, therefore, US national security. The structures needed to support the rapid development of capabilities are in place. However, the arduous process of innovation demands patience as these platforms emerge and disrupt the status quo of research and development (R&D) and procurement within government contracting systems of national security.

Take-aways from the Commercial Innovation System

Innovation can be taught and tracked. The enablers in the national security innovation base (NSIB) have been engaged in teaching and tracking innovation, but are still in the early stages of learning and applying lessons learned from private sector innovation systems.

Historically, government investments have been most useful for innovation generation and in basic research phases. Enabling can mean funding research and development, but just as important are the validation, feedback, and test and evaluation processes that flow from becoming an early customer, and the financial leverage that authentic government interest can stimulate.

When innovation enablers in the US federal government (such as those funding R&D) are willing to accept manageable risk, they can help spur innovation that might not be of significant interest to venture capitalists without government interest.

Having an idea is not enough. Developing ideas and scaling them so that they can spur an enduring customer response—whether for government (e.g., defense) or commercial purposes, or both—requires work and capital, which are influenced by time. Typical government contracting takes too long. Enablers that help accelerate the process can only work if government allows rapid transition to production and use (in some cases, this means getting out of the way).

Applying technological advances to defined mission sets also requires agility, and a willingness to change focus quickly. The concept of “failing fast” is just as relevant in national security ventures as in the commercial sector. In many cases, this means abandoning a direction, and allowing personnel and funding to move onto other important efforts without prejudice to status or careers.

These same concepts apply to the organizational structures that support innovation growth within the NSIB. Although tailored to the military service or mission they hope to innovate, these organizational structures must continually seek creative destruction as they collaborate with similar structures across the NSIB community, and tune their work toward greater impact.

INNOVATION

While many definitions exist, the commercial sphere recognizes innovation as the **creation and execution** of something new that provides real value for the customer, for which they will readily pay. Within the NSIB, we suggest that an operational definition of innovation is the **creation and execution** of something new that increases US national security, for which the government and its taxpayers agree to pay.

To date, some have confused **invention** with **innovation**. While both are certainly important elements, invention alone is not the rigorous process of turning a new idea into something of value.

A prime example of commercial innovation is the development of the smartphone: a single pocket-sized device that is a phone, calculator, word processor, web searcher, calendar, portable storage and gaming device, sensor suite, flashlight, and more. It accelerated the rise of a small personal computer firm (Apple) into a trillion-dollar company (in valuation) with global customers, thereby generating numerous competitors for both hardware and software elements.

An example of innovation in the national security sphere would be a transformative capability that renders a current threat harmless. As well, it could be a new weapon system that renders a prior class of attack systems obsolete. The military and intelligence agencies are customers of innovative solutions, as they acquire missiles, satellites, planes, ships, tanks, armaments, drones, and other tools to serve and sustain national security.

While the differences between the commercial and NSIB markets are clear, these markets share key elements that drive and develop innovation. Common to both are 1) innovators that found companies offering ideas and solutions, and 2) the constant search for capital and revenues to fund R&D and company growth during the embryonic phases. Such similarities are strongest in the need to progress to a self-sustaining revenue model as quickly as possible; to minimize expenses of early-stage development, and to beat competition to market.

A HISTORY OF DEVELOPMENT OF INNOVATION SUPPORT

The first VC firm, American Research and Development Corporation (ARDC) was formed in 1946 by Georges Doriot, a Harvard professor and naturalized French citizen who served in the US Army as a Brigadier General under General

Eisenhower's wartime push to harvest ideas from science and industry. ARDC's 1957 investment of \$70,000 for 70% of Digital Equipment Corporation (DEC) garnered \$35.5 million in 1969 at an initial public offering, 500 times the original investment, for an annual growth rate of 330%.¹

Figure 1. Innovation Structures in 2023

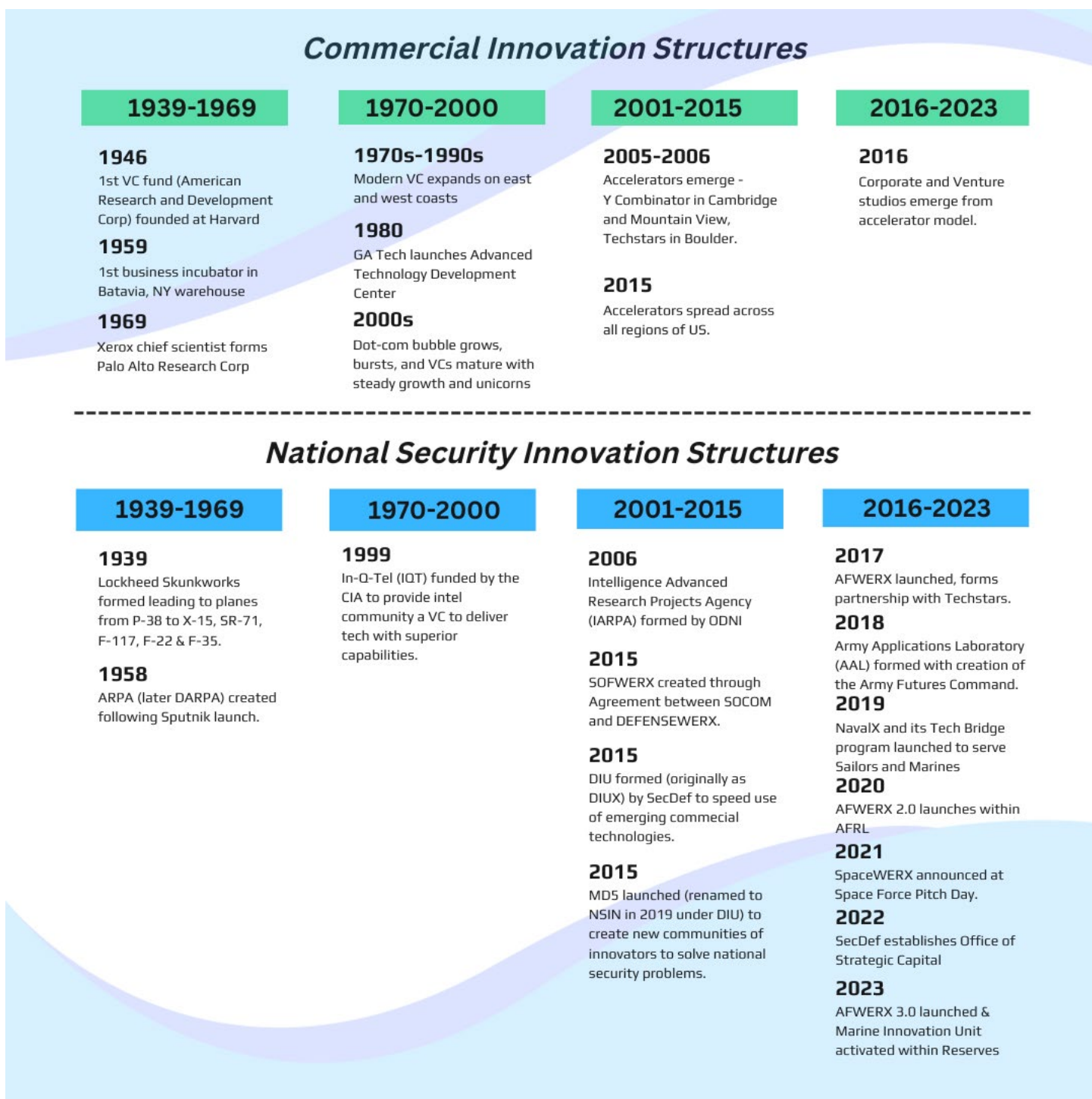
Innovation Structures in 2023		
Type	Global	US
VC Funds	27000+	12000+
Private Equity Funds	15000+	6000+
Angel Investors	3,000,000+	600,000+
Angel Investor Groups	4000+	95+
Tech Incubators	7000+	2000+
Technology Parks	5000+	1500+
Accelerators	5000+	2000+
Studios	850+	425+
Corporate Venture Incubators/Funds	3000+	1500+

In the 77 years since, the number of VC firms around the globe has grown to over 27,000, of which 12,000 are in the United States.² One of the most prolific and successful early-stage entities is Y Combinator. With offices in Cambridge, MA and Silicon Valley, CA, Y Combinator was formed in 2005 as an accelerator program that coached and funded select founders in groups (called cohorts) to create a cadenced stream of emerging tech startups. Another accelerator, Techstars, was founded in 2006 in Boulder, Colorado, and now has over 20 locations on 6 continents, providing mentor-driven coaching, as well as funding venues for early-stage technology companies that apply to join its cohorts. Figure 1 displays the many different types of innovation structures currently present in the commercial space.

In the national security space, the nation's first jet fighter, the 1945 Lockheed P-80 "Shooting Star" which became the fastest plane at the time, was developed in a separate engineering department that became known as the "Skunk Works." In 1958, the Advanced Research Projects Agency (ARPA, now DARPA) was formed in response to the surprise launch of Sputnik, with the explicit goal of accelerating innovative developments.

Figure 2 presents key milestones in the formation of structures within US commercial and national security markets that were created to harness speed and innovation. The

Figure 2. Key milestones in the formation of innovation entities.



growth in such structures since 2000 is notable, producing market-tailored entities that unite innovators, problems, ideas, prototyping, and funds to reduce time, risk, and cost to market.

THE ART OF DEVELOPING INNOVATION

Innovation as a process can be taught and learned. For example, Distinguished Professor Dr. Merrick Furst leads the “Deliberate Innovation” program at the Georgia Institute of Technology. Previously, Dr. Furst co-invented probabilistic circuit analysis and planning graphs, which are key breakthroughs in the field of AI planning. His work on innovation led him to found Flashpoint at Georgia Tech, an “accelerator studio” that draws on behavioral economics research to build “formative leaders and exceptional technology startups.”³ A primary lesson in such programs is that the discipline of innovation takes practice and patience to reduce risks and consistently achieve desired results.⁴

In the 2022 World Economic Forum ranking of innovation, four of the top five cities for innovation were in the US. In the ranking of innovation talent, the US had six of the top ten cities on the globe.⁵ The size of US free markets and the persistence of the innovator community continue to impress and influence world markets. However, both allies and adversaries of the United States are moving up in these rankings each year, spurred by the success of US elements of innovation in both commercial and defense applications.

COMPONENTS OF THE NSIB

Many of the underlying reasons for success of innovation in the national security environment relate directly to the strength of the individual components of the NSIB, which are here organized into three groups: enablers, innovators, and users/implementors.

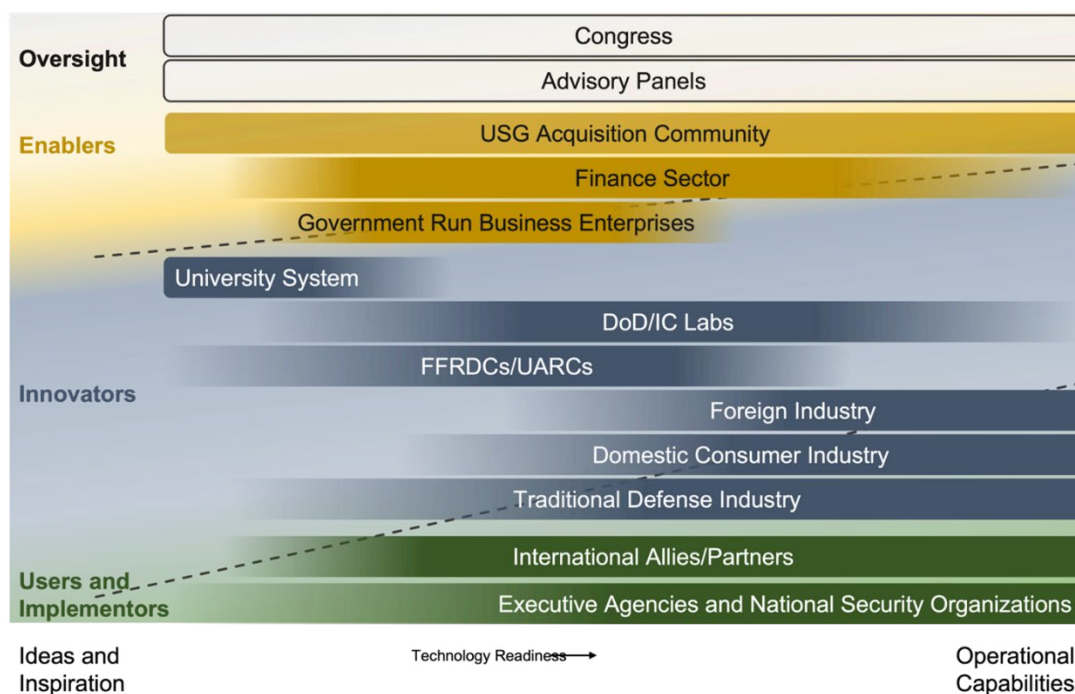
These are the entities that can benefit from lessons learned in the commercial innovation system. Figure 3 illustrates the kinds of entities in each group, and the degree of maturity in the development process that is the focus of each set of components.

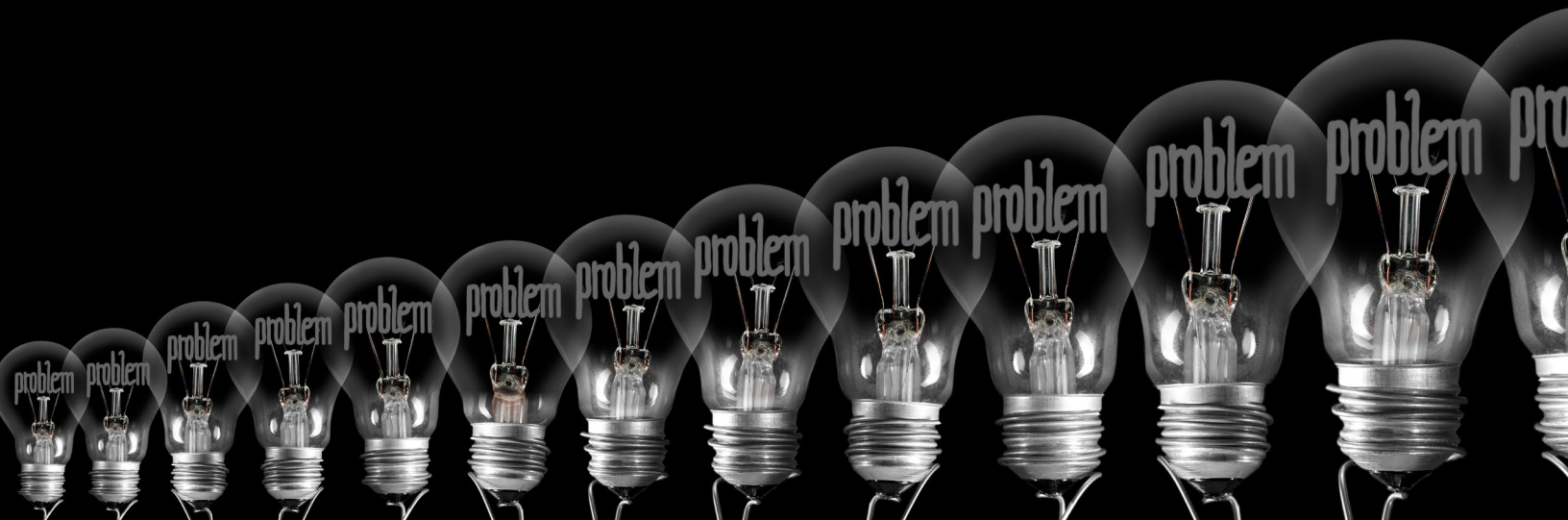
Enablers

The group of enablers is comprised of the entities that fund the NSIB, as well as organizations and individuals that catalyze the innovation process.

US Government funding for the NSIB comes from the US congressional authorizations and appropriations, and the DoD budget planning process, which generates requests to Congress in the President’s budget. These government funds provide R&D support to government employees and contractors throughout the nation, as well as to international allies and partners. However, the NSIB and its innovation enablers draw significantly more funding from investors through the nation’s public and private financial markets, including exchanges on Wall Street, private equity firms, and

Figure 3. Components of the NSIB





the world's first and largest VC and angel capital community. VC firms and angels not only provide the earliest and riskiest seed capital, but also continue to fund development and growth until profits can be generated. The VC and angel funds are integral to programming and mentorship at startup accelerators, incubators, and studios nationwide, including corporate accelerators and maker spaces engaged at several defense primes. Investments can target purely commercial applications, national security applications, or both. Other than government investors, investors generally do not have a market preference for how future profits will be generated.

In the commercial space, accelerators have launched and invested seed capital in over 10,000 startups across the economy.⁶ Moreover, their programming is so varied and strong that companies as diverse as Coca-Cola, Microsoft, JPMorgan, Comcast, and Stanley Black & Decker have used them to tailor innovation platforms for their respective sectors.

While it is true that most startups fail, failing founders will often start again in the same or a new market space. Much like the Army's Ranger School, this cycle creates a fast but powerful training ground for innovation leaders, which rewards success, but also values the experience and awareness that comes from failure followed by persistence.

Within the national security space, the government has been accelerating its structures for innovation enablers. In 2017, the Secretary of the Air Force announced a program called AFWERX to open "Air Force doors to highly innovative problem solvers with small amounts of money in ways that strip out bureaucracy."⁷ At the same time, it opened applications to the first cohort of its accelerator program, which was managed for the Air Force by Techstars.⁸

In 2020, three core activities were shaped within AFWERX: Spark, Prime and an integrated fund named AFVentures. By 2023, AFWERX presented its 3.0 model, as a directorate of the Air Force Research Laboratory, with an annual budget of over \$1 billion to accelerate change in the Air Force, focusing on the department's "Operational Imperatives" and fielding capabilities: "linking them to the procurement funding necessary to turn these projects into delivered capability at scale."⁹

Today, all US military services run accelerators. Examples of these organizations are AFWERX, CATALYST, MIU, NavalX, SOFWERX, SpaceWERX, and XTech. Other structures have been created to organize responses to specific challenges, such as the Department of the Air Force's DAF-MIT AI Accelerator. Others identify and activate innovative service



members who can bring specific mission problems forward, and/or identify and engage university and venture groups working in science and technology with dual-use applications. This is the focus of the National Security Innovation Network—the NSIN (formerly the MD5 Accelerator).^{10,11} In many of these organizations, military end users collaborate directly with technology entrepreneurs and their firms to both communicate warfighters’ priority technology needs and discover and develop emerging technologies. This is a remarkable expansion of government endorsement of innovation development for national security purposes.

As these accelerators and other structures were established, the DoD tested and launched a comprehensive defense-focused VC fund, the Defense Innovation Unit (DIU), that is run by a VC team with offices in Silicon Valley, CA; Washington, DC; Austin, TX; Boston, MA; and Chicago, IL. At the close of FY 2022, DIU’s annual report presented 17 prototype contracts to commercial firms that transitioned during the year to follow-on contracts with defense customers across DoD, with a potential production value of \$1.3 billion. This brings the total since 2016 to 52 transitions. Of these, 16 have transitioned into a Program of Record across multiple Program Executive Offices (PEOs). In total, DIU reports leveraging \$30

billion in private investment, with \$4.9 billion in production contracts to commercial firms, starting with 359 awards for prototypes.¹² After substantial increases in the DIU budget in FY 2023, there are proposals for a greater increase in FY 2024, potentially providing over \$1 billion in appropriations.¹³

With the start of a new fiscal year, DIU announced its 3.0 program under new director Doug Beck, a former Apple global VP.¹⁴

We will be a fast follower where market forces are driving commercialization of military-relevant capabilities in trusted artificial intelligence and autonomy, integrated network system of systems, microelectronics, space, renewable energy generation and storage, and human-machine interfaces.

—2022 National Defense Strategy¹⁵

Thirty days after the release of the 2022 National Defense Strategy, the Secretary of Defense announced the creation of the Office of Strategic Capital to integrate efforts across DoD to “develop, integrate, and implement proven partnered capital strategies to shape and scale investment in

critical technologies.”¹⁶ This new initiative is yet another demonstration of the consistent support for the unique service-specific innovation entities and the newly emergent DoD structures across the Secretaries of Defense in multiple administrations. The detailed study and stature of the Defense Innovation Board lends credence to the findings and recommendations embodied in its Strategic Investment Capital Task Force report of July 2023 entitled “Terraforming the Valley of Death.”¹⁷

Innovators

The group of innovators is comprised of scientists, engineers, university professors and students, entrepreneurs, corporate innovators, members of the military services, DARPA contractors and integrated defense firms, defense agencies, national labs, FFRDCs, UARCs and non-profits. These innovators advance ideas into innovations through experimentation, development of technology, and customer discovery to determine the product and market fit.

At present, innovators are likely to be concentrated in university campuses, technology parks, and business organizations in R&D, and internal Skunkworks groups, as well as in non-obvious places like planning and budgeting organizations. Virtually anyone who is capable of identifying, analyzing, and developing tentative solutions to a problem can become an innovator. Most importantly, innovation can be taught.

Across the economy and among corporate market leaders, thriving innovation programs actively work to discover “the next great thing” for growth as well as survival. The signs of creative destruction are often visible in these programs, including the very units charged with causing innovation. Innovators can develop applications for commercial markets, national security markets, or both. However, there is competition for innovation talent, as true innovators are rare.

Users and Implementors

Users and Implementors are the customers for NSIB innovation. They consist of integrated defense firms, contractors, the military services, and other defense groups applying technologic innovations to mission needs of the warfighter. This is the category where the problems are known and often painfully experienced. Thus, innovators should seek out these organizations as the primary customers for the solutions to problems encountered by end users.

ACHIEVING SCALE

Just as private companies seek to grow and scale their business through innovation, the NSIB also seeks to achieve scale in discovery, development, and application of innovation to national security. As decades of trial-and-error testing have shown, innovation can be deliberate and scaled.

Key indicators of organizations that are preparing to scale are *measurement, experimentation, self-examination, clear priorities, open communications, and transparency*.

These indicators might seem basic, but they are directly tied to recognition of how and to what extent the organization is on its path to scale. Specific technologies and capabilities must be protected in these early stages. However, the ability to rapidly court their transition from R&D through prototype, to conversion into acquisition programming requires collaboration and communication. These skills are essential to the knowledge base that will help the NSIB find innovation at scale.

The interactions of enablers, innovators, and users combine to produce innovation for the NSIB. Innovation at scale requires increased interaction among these three groups. In the commercial marketplace, major US cities feature multiple accelerators, university incubators, and private tech studios, along with multiple VC firms collaborating and competing in local markets. California’s Silicon Valley and Bay area are especially vibrant ecosystems that are home to over 1,000 VC firms. New York City has approximately 120 VC firms. Virtually all innovation hubs also have entrepreneurial universities and innovation support structures.^{18,19} Similar hubs exist throughout the nation and the world.

AN EXAMPLE OF SCALING

While it is not often recognized, many of these hubs owe their initial development to government initiatives. Many innovations, at least historically, begin with government needs. In many cases, commercial spin-offs overtake national security developments. For example, in 1993, Congress provided DARPA with funds to close the gap with other nations in the emerging global competition for technologies to build electric vehicles (EVs).²⁰ The project formed regional consortia of small and large businesses, universities, and national labs. The Congressionally directed program aimed to accelerate electric and hybrid-electric vehicle development in the United States with dual-use benefit to the US military.²¹ At the time, many military ground vehicles used

increasing amounts of electrical power for communications and command and control systems, and it was recognized that electric propulsion (in place of internal combustion) would reduce heat signatures and solve other problems for missions. It was also recognized that there would be commercial spin-offs and markets that could help reduce costs to the military market. Subsequently, the development program transitioned to the US Department of Transportation.

At the time, electric drive technology was far from ready for production. Among many challenges was the lack of sufficient power electronics to handle battery charging and discharging, and to control the compact and strong electric motors required for propulsion. The chips needed to make those switching decisions had not yet been designed, and many other supporting technologies needed further domestic development.

Today, the EV market is expanding rapidly worldwide. To reiterate, it is rarely recognized that government funding helped establish the groundwork for some of the technologies that would be required to allow companies to design and build EVs. Only when the market was ready and large enough to make production possible did production begin for consumer purchases. Before the latest consumer electric drive sedans and SUVs, there were prototype hybrid-electric Army Humvees and M113s. Additionally, production of electric and fuel cell-based commercial buses, garbage trucks, and tractor-trailer rigs evolved from the government programs in the United States and within allied markets at major firms.^{22,23} A healthy competition for component supply and sourcing (including for lithium-ion batteries) developed around the globe. Without those investments at the time, the emergence of viable consumer EVs might have been further delayed.

One aspect of the government program was crucial to the rapid R&D required to establish key technologies. DARPA employed its Other Transactions Authority (OTA) to contract with regional consortia that managed a diverse portfolio of projects through teaming agreements tied to the OTA structure. With quarterly payments for clear team milestones, funding flowed with progress, and failing projects were quickly shuttered with unspent funds redirected to next-priority projects. Today, other transaction agreements have become far more prevalent, with increasing interest and acceptance within the DoD and other agencies, and encouragement from Congressional authorizers and appropriators. There have been numerous amendments to the law

for OTAs in the years since Congress first authorized them for NASA in 1958, culminating in the current Sections 4021 and 4022 of title 10 of the US Code.^{24,25, 26}

As EVs emerge on global markets, there is no doubt that the technologies have spread worldwide, and that now US firms are in a global race to dominate markets. EV factories exist in the United States, Europe, and especially Asia. However, it is not certain that the United States capitalized on its technology investments as rapidly as possible. Thus, another important aspect of innovation is to be first to find a repeatable market for ideas and technology because ideas are rarely unique or protected for long.

NEXT DIRECTIONS

The list of NSIB enablers continues to grow. In December 2022, the Secretary of Defense announced that the Office of Strategic Capital will “scale investments” between existing innovation units, and to increase “the capital available to critical technology companies to help them reach scaled production.”²⁷ The DIU is undergoing transformation with the appointment of a new director from a private sector mega-cap tech firm, higher reporting visibility, and a significant increase in funding proposed for FY 24. DARPA, the Services, other organizations within DoD, and other government agencies from NASA to the Department of Transportation are making greater use of OTAs to speed contracting and facilitate research advancements.

The US government needs to redouble efforts to track the successes and failures of innovation programs. While contracting tools such as SBIRs, STTRs, and OTAs are building momentum, new tools should be developed. Various authorities in place since the 1950s that are not working need to sunset, while successful enablers of innovation need strengthening. OTAs have earned a respected seat at the acquisition table, and Congress has been gradually expanding their applicability. However, current cost-share requirements in research OTAs inhibit their use in the often-risky basic research arena, where an innovative idea is farthest away from potential revenue generation. DARPA might be a good resource to experiment with lifting this requirement, especially in areas of critical national security need.

The government should also streamline its approach to using loan guarantee authorities to encourage private sector lending into the capital stack of rapidly growing innovative firms in the NSIB. This is particularly the case for hardware

intensive **innovations** that are capital intensive, as these can accelerate development and transition. Historically, **loan guarantee authorities** have successfully been used in defense industrial base applications in the past, including for Lockheed's development and initial production of the C-5 Galaxy aircraft. These **authorities** have also been utilized for emerging technologies to address climate change. For example, the DOE Loan Program Office provided financing **to quickly build new EV factories** for Tesla and Ford as well as battery plants **to supply EV manufacturers**.

Since the pursuit of innovation in national security is tied to addressing near-peer challenges, increased funding for successful innovation programs is warranted. But programming steady increases may be more manageable and defensible than large leaps that create programmatic bullseyes. The work of building top-tier project portfolios is difficult and time-consuming. Predictable funding levels are vital to the ability to rapidly execute initiatives and program transitions.

Each of the Services and agencies with innovation structures must calibrate their mission to the intended users. The goal is to foster innovative capabilities, rather than moving money, or merely counting the number of grants, contracts, and agreements. Measuring outcomes requires patience in assessing capabilities, and persistence in pursuing promising concepts, including assessing means to scale the capabilities for production.

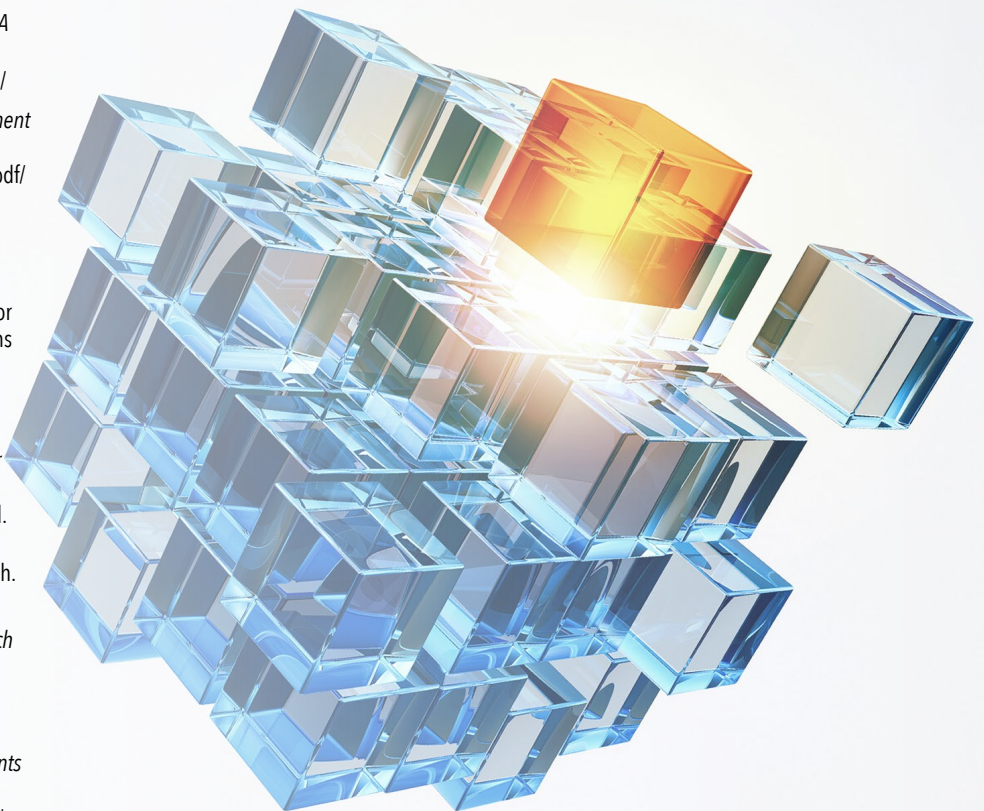
Today, DoD, the Services, and the Intelligence Community are accelerating the tempo of funding, review, change, and execution across their portfolio of innovation organizations. This form of creative destruction is a healthy indicator of these programs' maturity. Acquisition tools (including OTAs) are helpful, but still insufficient to the challenge of compressing time scales. The NSIB needs to mirror what has transpired in the global commercial sector cadenced to the challenges outlined in the National Security Strategy. Most importantly, these nascent structures for the national security sector should adapt models developed in the commercial innovation space to the particular needs and missions of their parent organizations, and should utilize appropriate lessons learned (both positive and negative), from experiences in the commercial arena, especially as related to the need for speed to market.

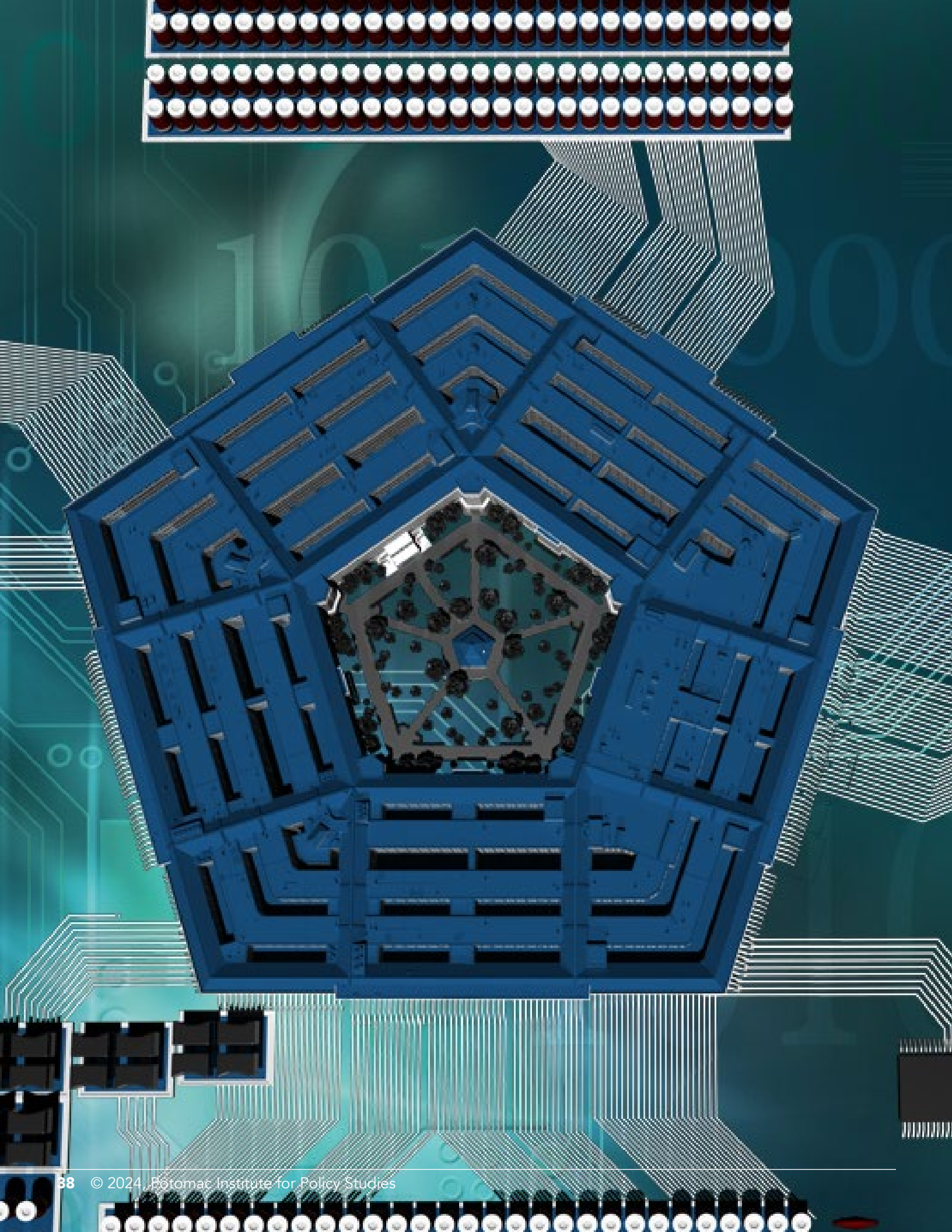
Such lessons include discovery that innovation can be taught, and that it is important to track progress as innovations are developed, modified, and scaled. And finally, one must execute fast, fail fast, regroup quickly, and persevere.

REFERENCES

- 1 Katie Macdonald, *Venture Capital, History Cambridge, 146 Sixth Street (Location of Ionics)*, Innovation in Cambridge, Cambridge Historical Society, 2012, <https://historycambridge.org/innovation/Venture%20Capital.html>
- 2 National Venture Capital Association, <https://nvca.org>; CB Insights, <https://www.cbinsights.com>; Angel Capital Association, <https://www.angelcapitalassociation.org>; Pitchbook, <https://pitchbook.com/venture-capital-database/>; Global Startup Ecosystem Report, Startup Genome LLC, 2022, <https://startupgenome.com/reports/gser2022>
- 3 Georgia Tech, Center for Deliberate Innovation, <https://cdi.gatech.edu/index.html>
- 4 Flashpoint, *The Trillion Dollar Opportunity - Keynote | Merrick Furst* [Video], YouTube, Jun. 1, 2018, <https://www.youtube.com/watch?v=O8rzmRAppws>
- 5 Kayleigh Bateman, *Which are the world's most innovative cities in 2022?*, World Economic Forum, Feb. 02, 2022, <https://www.weforum.org/agenda/2022/02/innovative-global-cities-talent-property/>
- 6 Sergio Paluch, *Top 40 Startup Accelerators Based on Data - Updated for 2023*, Beta Boom LLC, 2022, <https://betaboom.com/blog/best-startup-accelerators/>
- 7 Secretary of Air Force Public Affairs, *Air Force opens doors to universities, small businesses and entrepreneurs to boost innovation*, US Air Force, July 21, 2017, <https://www.af.mil/News/Article-Display/Article/1254932/air-force-opens-doors-to-universities-small-businesses-and-entrepreneurs-to-boo/>
- 8 Secretary of Air Force Public Affairs, *Air Force opens applications for dual-purpose technology accelerator program*, US Air Force, Sept. 15, 2017, <https://www.af.mil/News/Article-Display/Article/1313455/air-force-opens-applications-for-dual-purpose-technology-accelerator-program/>
- 9 Katie Milligan, *DAF transitions from AFWERX 2.0 to 3.0 during livestreamed event*, The Air Force Research Laboratory, Dec. 14, 2022, <https://www.af.mil/News/Article-Display/Article/3245893/daf-transitions-from-afwerx-20-to-30-during-livestreamed-event/>
- 10 Acquisition in the Digital Age, *Understanding DoD: Tap the Innovation Ecosystem*, MITRE Corporation, 2023, <https://aida.mitre.org/demystifying-dod/innovation-ecosystem/>
- 11 National Security Innovation Network, *MD5 Adopts New Name to Reflect Refined Mission*, U.S. Department of Defense, May 06, 2019, <https://www.nsin.mil/news/2019-05-06-md5-adopts-new-name/>
- 12 Defense Innovation Unit, *Sneak Peek: DIU's FY2022 Year-In-Review*, U.S. Department of Defense, Dec. 13, 2022, <https://www.diu.mil/latest/sneak-peek-dius-fy2022-year-in-review>
- 13 Courtney Albon, *House eyes billion-dollar 'hedge portfolio' to push commercial tech*, C4ISRNET, Jun. 23, 2023, <https://www.c4isrnet.com/battlefield-tech/2023/06/23/house-panel-eyes-billion-dollar-pentagon-fund-to-push-commercial-tech/>
- 14 Lauren Williams, *The Pentagon's innovation arm has a new chief and a new strategy*, Defense One, Sept. 01, 2023, <https://www.defenseone.com/technology/2023/09/pentagons-innovation-arm-has-new-chief-and-new-strategy/389948/>
- 15 C. Todd Lopez, *DoD Releases National Defense Strategy, Missile Defense, Nuclear Posture Reviews*, U.S. Department of Defense, Oct. 27, 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3202438/dod-releases-national-defense-strategy-missile-defense-nuclear-posture-reviews/>
- 16 U.S. Department of Defense, *Secretary of Defense Establishes Office of Strategic Capital*, Dec. 1, 2022, <https://www.defense.gov/News/Releases/Release/Article/3233377/secretary-of-defense-establishes-office-of-strategic-capital/>

- 17 Defense Industrial Board Task Force Report, *Terraforming the Valley of Death*, July 17, 2023, https://innovation.defense.gov/Portals/63/DIB_Terraforming%20the%20Valley%20of%20Death_230717_1.pdf
- 18 Crunchbase, *San Francisco Bay Area Venture Capital Companies*, 2023, <https://www.crunchbase.com/hub/san-francisco-bay-area-venture-capital-companies>
- 19 Nicolás Cerdeira, *Top 50+ Venture Capital Firms in New York in 2023*, Failory, August 25, 2023, <https://www.failory.com/blog/venture-capital-firms-new-york>
- 20 Electricore, *History and Background*, 2016, https://www.electricore.org/history_and_background_
- 21 The Center for Transportation and the Environment, *DARPA Electric and Hybrid Electric Vehicle Program*, <https://cte.tv/project/darpa-electric-and-hybrid-electric-vehicle-program/>
- 22 DTIC, *Final Report, Electric Drive M113 Vehicle Refurbishment Project, Sacramento Electric Transportation Consortium RA93-23 Program*, Feb. 1997, <https://apps.dtic.mil/sti/tr/pdf/ADA322403.pdf>
- 23 The Center for Transportation and the Environment, *Our Members*, <https://cte.tv/about-us/our-members/>
- 24 The author founded and directed one of these consortia for eight years, followed by the deputy director who today runs the renamed Center for Technology and Environment. The Center for Technology and Environment, <https://cte.tv>
- 25 Rhys McCormick and Gregory Sanders, *History of the DOD's OTA Powers, Trends in Department of Defense Other Transaction Authority Usage*, Center for Strategic and International Studies, May 2022, https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220525_McCormick_Trends_OTA.pdf?VersionId=JrTKXLxEFSrSGQh.CaObBZnbZAJkWZ.i
- 26 Legal Information Institute, *10 U.S. Code § 4021 - Research projects: transactions other than contracts and grants*, Cornell Law School, <https://www.law.cornell.edu/uscode/text/10/4021>
- 27 Edward Graham, *DoD Creates Office to Enhance Investments in Tech Vital to National Security*, Nextgov/FCW, Dec. 02, 2022, <https://www.nextgov.com/emerging-tech/2022/12/dod-creates-office-enhance-investments-tech-vital-national-security/380420/>







TRUSTED ACCESS TO MICROELECTRONICS

*Addressing DoD's Unique Issues
of Accessibility, Integrity, and
Confidentiality of Microelectronics*

Ted Glum, Member of the Board of Directors,
Potomac Institute for Policy Studies

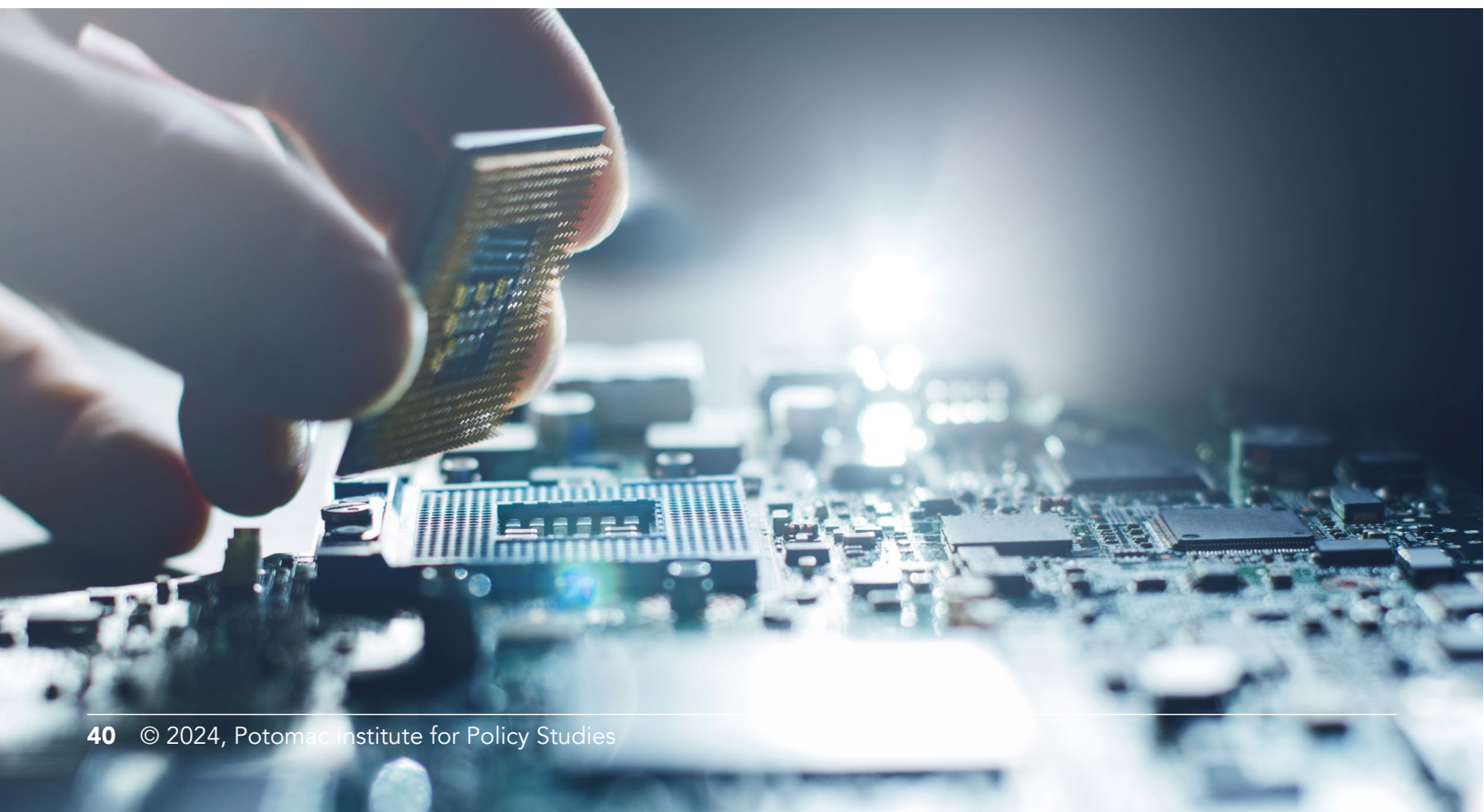
With all the current emphasis on the supply chain issues for microelectronics, as well as the CHIPS Act's attempt to re-shore production, it is worth considering the unique needs of the US Department of Defense (DoD). The DoD needs access to both commercial-off-the-shelf (COTS) microelectronics and trustworthy devices for its weapon systems and operations. The US military has long depended on electronics, and modern defense systems increasingly rely on the superior performance of microelectronics to sense, decide, adjust, control, and act.¹ Whereas in the past, the best defense was to have the most firepower and best armor, now a modern defense depends on superior microelectronics.

This dependence is why the US DoD has long been concerned with "trusted access" to microelectronics. Trust means different things in different contexts, but here we adopt an inclusive understanding of trusted access in three dimensions:

- **Accessibility** refers to the ability to obtain and use the required microelectronics when needed. For example, in wartime, the Department might need to produce many weapon systems rapidly. Production delays due to microelectronics supply limitations would operationally compromise the military.
- **Integrity** refers to the trust that the microelectronics serve their intended functions and that no other functionality such as a kill switch, backdoor, or data capture was inserted covertly.
- **Confidentiality** of the microelectronics relates to trust that competitors and adversaries cannot glean information to compete with or defeat a system based on their knowledge of the design or type of microelectronics. This dimension of trust includes security against major vulnerabilities such as rival access to proprietary or classified knowledge of a microelectronic part's intended use (or even the customized design of those parts).

Critical infrastructure industries, such as companies involved in the electric power grid, cloud services, and banking, are concerned with trusted microelectronics to ensure the integrity and reliability of their systems. Producers and consumers of commercial products, such as automobiles, similarly have an interest in the accessibility and integrity of their constituent electronics, if not also confidentiality. But the military has a particular interest in a high level of trust across all three dimensions because adversaries are motivated to attack these attributes. Thus, microelectronics used in all these areas need reliable access to trusted parts with the assurance of some degree of accessibility, integrity, and confidentiality of the supply.

The COVID pandemic highlighted the vast regional concentration of microelectronics production in Asia, exposed the fragility of the microelectronics supply chain, and revealed the vulnerability of microelectronics parts to malicious intent.² Recently, there has been much focus on the fact



that a large percentage of the microelectronics used in the US, including by the DoD, are manufactured, assembled, and tested overseas. While the CHIPS portion of the CHIPS and Science Act of 2022 will attempt to re-shore American microelectronics manufacturing, it will not automatically guarantee access to trusted microelectronics. American fabrication alone will not ensure that microelectronics are free of defects, malware, inserts, or spyware.

The Department has a long history of providing support and services to DoD industrial suppliers to ensure that microelectronics are trusted, as defined in this paper. The program, generally known as the **Trusted Foundry** program, has evolved over time, addressing the issue of trust for parts over the entire range of the microelectronic supply chain (design, fabrication, packaging, and testing) to include guaranteed access, integrity, and confidentiality.³ The program’s name, the Trusted Foundry program, is a misnomer because the program goes far beyond foundry services and has led to confusion over what this program provides and the gaps (including those in the CHIPS Act) that it hopes to fill.

DOD ACQUISITION OF MICROELECTRONICS

The US DoD accesses a wide variety of microelectronic parts for use in defense systems through its many contractors and suppliers. Defense needs include new and emerging technologies (e.g., silicon photonics), state-of-the-art (SOTA) technologies (currently 7nm and smaller), state-of-the-practice (SOTP) mature microelectronics (typically 28 to 45nm), and legacy technologies (nodes greater than 45nm or other parts no longer in production or readily available for purchase). In addition, the DoD requires that parts satisfy significant qualification criteria against unique operational demands, such as challenging battlefield conditions and radiation hardening for space applications.

State-of-the-Art (SOTA)	Currently 7nm or less
State-of-the-Practice (SOTP)	Typically, 28 to 45nm
Legacy parts	Larger than 45nm, sometimes microns, generally no longer in production

DoD programs generally have lifetimes far outlasting the life cycle times of typical commercial microelectronics parts. Sustainment cannot be based on the assumption

that subsequent generations of parts will enable backward compatibility. Access to parts no longer in production (legacy parts) is an all-too-common problem for the DoD who generally rely on prime contractors and their subcontractors to ensure long-term access to needed microelectronics for their systems. Primes and their subcontractors must worry about when manufacturing sources have been discontinued or have moved on to new generations of electronics. This process is called “Diminishing Manufacturing Sources and Material Shortages Management”—or “DMSMS management.” Mitigation of microelectronics DMSMS is a particularly vexing problem for the DoD.

When the parts become outdated, systems must still be maintained as originally designed. Upgrades involving tech redesign are extremely costly. Given the pace of microelectronic advancements, the cost of redesigning based upon the constant evolution of each type of microelectronic device used in a system is not budgetarily feasible. In addition, each redesign must proceed through a systematic progression of time-consuming systems testing and re-qualification. In short, although redesigns are beneficial by using newer technology, these redesigns must be programmed, budgeted, and scheduled for testing and integration into operations. These block cycle upgrades could be shortened and cycled more often using digital engineering and open system architectures. However, in systems highly populated with microelectronics, these cycles should be generated from a managed upgrade plan and sustainment practices, not from a reaction to a single DMSMS notice.

DMSMS mitigation of every single device in every system is not practical. Therefore, each new system requires a plan for long-term sustainment to include a long-term supply of devices as originally designed and a plan for tech insertion via programmed redesigns.

Acquisition of microelectronic parts that are currently in production (i.e., state of the art—SOTA and state of the practice—SOTP) can also present issues for the DoD. Suppliers delay or fail to fulfill orders for parts due to the low volumes DoD requires for production. Commercial orders involve much larger volumes, so it is generally not economical for a commercial microelectronics supplier to process low-volume orders.

Export control compliance and International Trafficking in Arms Regulations (ITAR) further complicate procurement due to the need to provide specifications for required parts. Regulations may prohibit companies from providing

explicit requirements, so companies must find alternate sources or hide intended end-use through multiple layers of obfuscated procurement companies. Export control regulations sometimes inflict net harm on systems procurement instead of providing the protections the regulations were meant to provide.⁴

Regardless of the reason, DoD and the Defense Industry has very little insight into its systems' entire microelectronics supply chain. Subassemblies, constituent parts, and manufacturing steps can be five to twenty tiers below the prime contractor, and all the various sources can be impossible to track.

The result is great uncertainty about the integrity and long-term supply needs of microelectronics for the DoD, whether for legacy or currently produced parts. The DoD and the intelligence community (IC), in particular, require access to parts that provide high assurance that neither the design nor the purpose is revealed to potential adversaries. Ensuring this level of integrity and confidentiality requires extraordinary caution and chain of custody oversight.

HISTORY OF TRUSTED ACQUISITION OF MICROELECTRONICS

Decades ago, the government set up its own microelectronics fabrication facility (a "fab"), run by National Semiconductor, located on secured federal property, and dedicated to specific microelectronics production for government purposes. This dedicated fab eventually shut down because it was too expensive to continue to operate and upgrade without commercial use and because the facility became obsolete. In 2004, a new program called "Trusted Foundry" was initiated by the intelligence community (IC) to provide both guaranteed access to a then-state-of-the-art US fab at IBM along with a high degree of security. The **Trusted Foundry Program** was managed by an organization internal to the IC called the **Trusted Access Program Office** (TAPO). IBM was compensated with two contracts—one for access and multi-project wafer runs and the other for security services. While the TAPO organization managed these contracts, the costs were split between the IC and DoD offices in the Pentagon. The Defense Microelectronics Activity (DMEA) based in Sacramento was made the DoD program manager and funded to provide the DoD portion of the funding.

Around 2007, DMEA expanded the DoD portion of the program, still called the "Trusted Foundry Program" to include

formal accreditation and audits of other fabs and services needed to create an entire ecosystem of microelectronics suppliers with a high level of trust. These services included design, fabrication, assembly, and testing. The trusted set of microelectronic technologies now available for systems includes mature parts and some highly specialized processes. This accredited group of performers formed the **trusted suppliers group** as part of a **Trusted Supplier Program**.

Around 2014, IBM divested itself of its fabs to the company GlobalFoundries, with IBM paying GlobalFoundries in this contractual transaction to offload its then-unprofitable microelectronics fabrication business. GlobalFoundries had major ownership investments from the United Arab Emirates, so the "sale" required approval from the US Committee on Foreign Investment in the United States (CFIUS). CFIUS required that the contracts were novated and continued to be executed with appropriate security for "GlobalFoundries US" under a proxy Board of Directors consisting of approved US citizens.

In 2016, as the initial contracts were nearing their end, the IC turned over the management of the entire Trusted Foundry Program to DoD. DMEA assumed the IC's TAPO responsibilities and created a new TAPO entity within DMEA with the combined program consisting of the Trusted Supplier Program and the trusted foundry contracts. These combined efforts were still called the Trusted Foundry Program, despite including multiple activities beyond simple trusted foundry access. After a re-compete, GlobalFoundries US retained contracts to supply access to the latest microelectronics technology as part of the expanded Trusted Foundry Program.

In 2018, GlobalFoundries made a business decision to offer only prior node geometries and not to attempt to keep up with the latest smaller geometries (smaller than 12nm), which would require billions of dollars in new investments. As a result, the TAPO contracts managed by DMEA could no longer guarantee access to trusted SOTA microelectronics, although they could supply the DoD needs for trusted mature technologies at nodes and geometries greater than 12nm.

GlobalFoundries' business decision reflected worldwide market conditions for microelectronics, resulting in the concentration of SOTA fabrication (now at geometries smaller than 12nm) in Taiwan and South Korea. This challenged the Trusted Supplier Program because the approved trust accreditation model only allowed for companies fully owned

and operating in the “five-eyes” nations (US, UK, Canada, Australia, and New Zealand).

The Trusted Foundry Program and TAPO nonetheless continue to supply accredited SOTP trusted parts and services to the DoD, despite the global migration of SOTA fabs to Asia, making trusted SOTA parts by any program unfeasible.

CURRENT CAPABILITIES

The Trusted Foundry Program continues to provide accredited secure services, including SOTP fabs (producing the most utilized parts within the DoD), albeit currently without the ability to provide accredited trusted parts at nodes below 12nm. The Trusted Supplier Program as part of the Trusted Foundry Program accredits all “trusted suppliers” in the microelectronics domain according to well-defined, auditable criteria. Trusted suppliers include not only foundries but also trust-accredited suppliers of design tools, ASIC design services, packaging and testing, assembly, prototyping services, or other stages in the development and manufacture flow of electronics for DoD systems. DoD programs use accredited suppliers, generally by direct interaction between the program’s industry contractor(s) and their chosen accredited supplier. The requirement for the use of accredited suppliers flows from DoD policies as adjudicated by each program office and is often part of the customized “Program Protection Plan.” Trust can also include protection of industry proprietary rights and security protection. The Office of the Secretary of Defense can issue waivers when necessary.

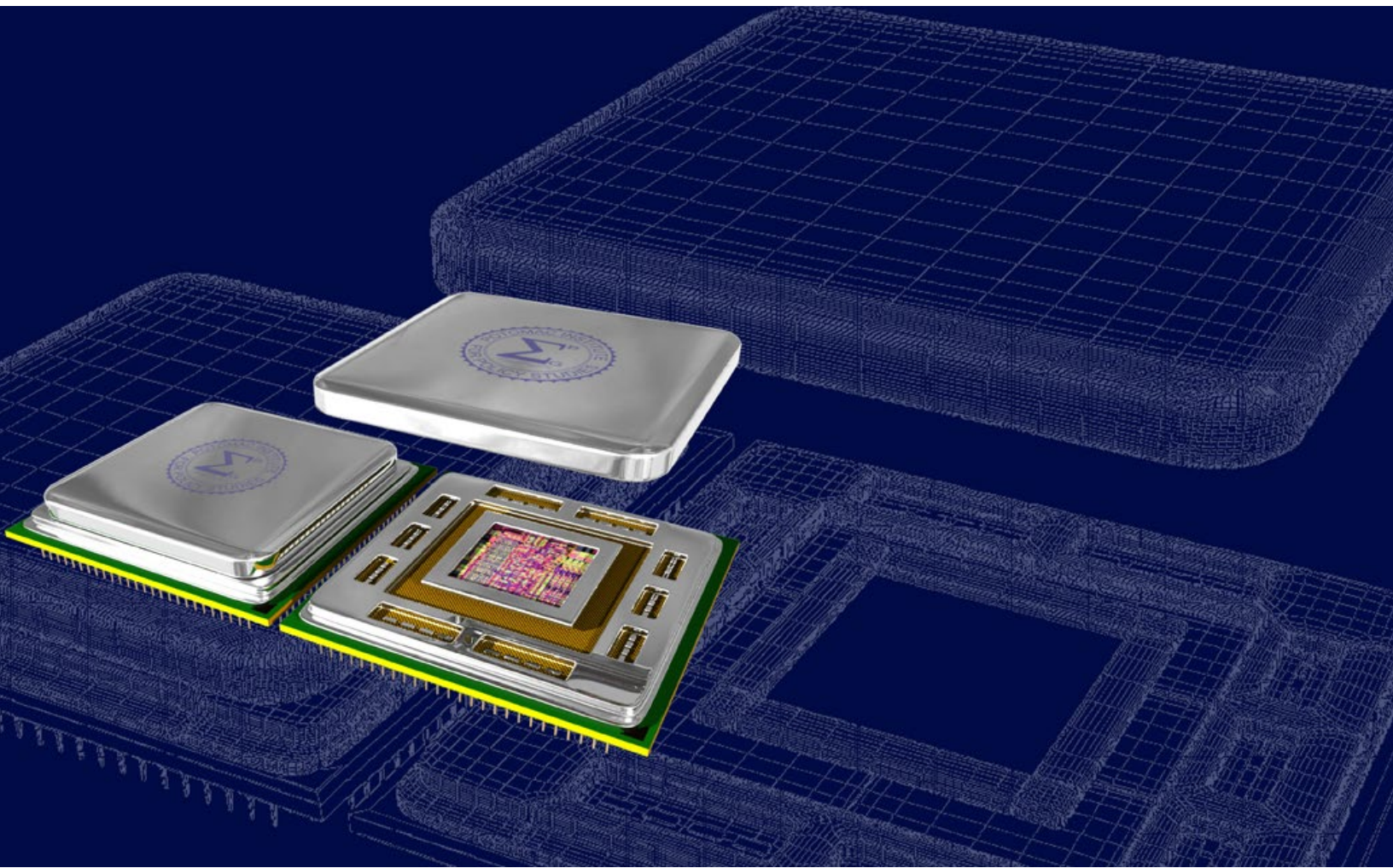
Still administered by the DMEA, the TAPO continues to provide DoD programs with access to microelectronics and electrical components that include a high degree of trust. GlobalFoundries US continues to have special contracts for access to their facilities giving TAPO priority access for runs involving multi-project wafers. These runs help solve the access issue for DoD by providing low-volume supplies for DoD programs and corporate research projects. A key to addressing the access issue caused by the economic preference for mass production runs is the aggregation of multiple requests from different projects onto a single wafer and executing the run through the trusted GlobalFoundries US fab. The TAPO contract for this trusted foundry includes pre-negotiated volume discounts for production at various breakpoints, paid for by the program offices requiring the parts. At this time, the technologies provided by GlobalFoundries allow for custom-designed

devices necessary for US traditional and irregular warfare requirements. These technologies align with current DoD program needs but are already a few generations behind commercial SOTA. Nonetheless, highly qualified technologies can be integrated into critical national security programs, thus increasing the performance level of our systems.

TAPO processes can provide design tools to support DoD programs, providing proprietary intellectual property (IP) microelectronics components based on enterprise-wide licenses for current and legacy part designs. Security measures permit runs that support commercial proprietary, ITAR-restricted, Export Administration Regulations (EAR)-restricted, and trusted processing up to the Secret level.⁵ TAPO can also provide microelectronics consultative support to DoD contractors using microelectronics experts and acquisition professionals cleared to the Top Secret/Sensitive Compartmented Information level.

In some cases, weapon systems must be sustained by producing small volumes of parts that replicate the form, fit, and functionality of obsolete COTS components. The Defense Logistics Agency has the Generalized Emulation of Microcircuits (GEM) program, and DMEA provides the Advanced Reconfigurable Manufacturing for Semiconductors (ARMS) program to address these needs.

Currently, 81 suppliers are accredited.⁶ One of these is the GlobalFoundries “trusted foundry” and provides the highest level of trust. The remaining suppliers provide greater trust than buying commercial-off-the-shelf microelectronics. TAPO guides the use of accredited facilities,⁷ but their use is the responsibility of the (defense) industry and the industry’s program executive office. DoD programs can either encourage or require that their contractors use only accredited suppliers for their microelectronics needs, which can include design, multi-project wafer run aggregation, mask data preparation, mask manufacturing, wafer fabrication, dicing, packaging/assembly and testing, and customer support services. The use of accredited suppliers reduces vulnerabilities from supply disruptions or malfeasance. This proven methodology provides pre-approved and accredited suppliers which ensures a well-defined and audited trusted supply before manufacture starts, without time intensive, after-the-fact reviews of each part that could result in years’ long delays of program development. It is important to note that to date (over 15 years), **no known malicious parts have come from the DMEA-accredited trusted suppliers.**



THE CHIPS AND SCIENCE ACT

During the peak of the COVID pandemic from 2020-21, microelectronics supplies for key industries, including automobile manufacturing, became limited. The auto companies canceled existing orders fearing a long downturn in demand. When production needed to ramp up due to unforeseen renewed demand, auto manufacturers had to delay production because of tight supplies. This circumstance was a wake-up call to policymakers who realized that commercial industry vulnerabilities due to foreign source dependencies and long supply chains will surely result in even more vulnerable defense industries. The defense industry relies on low volumes of specialized chips, which means that defense is particularly vulnerable to supply disruptions. Worse, foreign suppliers from adversary countries might be motivated to tamper with electronics intended for US weapon systems, especially for customized chips whose use is exclusive to defense applications.⁸

The Trusted Foundry Program, with its proven Trusted Supplier Program, ameliorates the vulnerabilities, but gaps remain. The CHIPS and Science Act of 2022 attempts to remedy these challenges by stimulating domestic production. The Act incentivizes firms to build fabs and other microelectronics production facilities in the US. The Act also provides funding, primarily through the Department of Commerce, for research so that future facilities can keep up with the fast rate of development in the microelectronics field. The Act further provides for a research program conducted by the DoD, the “DoD Microelectronics Commons,” to stimulate development opportunities for researchers for specific DoD applications. The DoD Microelectronics Commons is intended to allow universities, small businesses, and industries to leverage fabs and design technologies to produce prototypes of microelectronics to serve DoD-specific needs.

The Act represents a bold attempt to strengthen a vital industry for US national security by using taxpayer funds

and tax incentives. But again, the fact that chips and electronic systems are built on US shores does not, by itself, guarantee trust. This is especially true for defense systems and US critical infrastructure. It also does not ensure that all future technologies will be produced domestically to serve all possible needs. Even if the goal of re-shoring microelectronics production was totally successful and domestic production served all needs, additional steps would be required to ensure trusted supplies to defense applications and critical infrastructure.

TECHNOLOGY DIRECTIONS

SOTA microelectronics fabrication has moved to 7nm and will soon progress to 3nm and 2nm designs. Other specialized technologies, such as Silicon-on-Carbon (SiC) and 3D packaging, provide non-scaling-based customized capabilities. Applications that require various technologies include communications and radio-frequency processing, optical applications, encryption applications, and microelectronics that will work on spacecraft subject to high radiation levels. While programmable microprocessors and other commodity microelectronic parts such as FPGAs can serve a large variety of needs, defense applications increasingly need customized microelectronics designed especially for their specific application. The DoD will need reliable access to trusted microelectronics that can serve these and other specialized applications.

TAPO 2.0

Today, TAPO is successful in accessing and supplying the trusted mature technologies that the DoD requires. In the future, defense systems will need the latest technologies to defeat adversary systems. Because SOTA fabs are currently concentrated in Asia, TAPO is constrained in supplying cutting-edge trusted microelectronics commodities. Defense systems will also need sustained supplies of legacy microelectronics that can be trusted.

The TAPO program run out of the DMEA has successfully addressed the issues of access, integrity, and confidentiality (i.e., trust) for the DoD for over 15 years without any known malicious parts coming from the TAPO's accredited trust program. This program can and should serve as a model and foundation to evolve into a TAPO 2.0 program. Such a program would combine CHIPS Act incentives to re-shore SOTA fabs to fill gaps in the trusted microelectronics supply chain with updated SOTA security protocols that take

advantage of the current, more highly automated environment of a SOTA fab. In this way, TAPO 2.0 would only need a "light touch" and low-cost overhead to source secure parts within a commercial fab. These protocols have been developed such that they can provide the level of trust needed largely within the commercial fab's manufacturing process without the expense of a dedicated, trust-only fab. This effort would fill the current SOTA gap of the Trusted Foundry Program. The primary missing piece—access and trusted parts from SOTA facilities—would be a focus of this expanded portion of a trusted access program.

The existing and proven Trusted Access Program provides the necessary ingredients but will need to expand as new facilities and new technologies are introduced. New facilities will need to be accredited, audited, and advised on maintaining trust—for example, to avoid being compromised by nefarious hacking or malware. Expertise will need to be expanded for consulting services for defense contractors based on new technologies and customization needs. DMSMS management functions will require the procurement of sufficient supplies based on long-term needs assessments. Developers and program managers for defense systems and critical commercial systems will need to be aware of the offerings with greater trust. In some cases, for national security purposes, the use of trusted facilities will need to be mandated. Multiple "tiers of trust," properly defined, will need to be developed and managed according to the applications.⁹

The process and protocols for accrediting facilities for trust and maintaining trust accreditation will evolve with the technologies. For some applications, facilities at international allies and partners (beyond the "five-eyes" partners) may be accredited.

WAY FORWARD

The CHIPS and Science Act sets in motion the possibility of providing more domestic supplies of microelectronics to serve US needs. However, trusted supplies are necessary for national security applications, assured access in times of need, critical infrastructure applications, and other purposes. The Act did not explicitly address trust issues.

Accordingly, going forward, several steps are needed, requiring government actions:

1. Expand the current highly successful and proven Trusted Foundry Program at DMEA to coordinate with the CHIPS

Act that will encourage re-shoring of microelectronic sources. The TAPO office will need to give rise to a TAPO 2.0 expanded accreditation program, which develops criteria for “tiers of trust” at various levels, provides counsel to suppliers, and oversees an expansion of suppliers that can provide trusted microelectronics and electronics based on all levels of production. The office will need to expand the “intellectual property” building blocks of trusted design components offered to developers in designing customized secure microelectronics. New forms of shared capabilities are needed to enhance aggregation services, including design software and hardware production. TAPO 2.0 will need appropriate resources to accomplish these new goals.

2. Ensure that new manufacturers benefiting from CHIPS Act incentives comply with TAPO 2.0 trust accreditation processes and meet national security needs. Newly incentivized US-based fabs and facilities should be required to attain a level of trust accreditation to serve US needs.
3. Require providers using microelectronics in society-level critical infrastructure to use trusted microelectronics as accredited by TAPO 2.0. While such a requirement is useful to increase the market for trusted microelectronics, it is necessary for the security interests of the nation and provides a viable economic market for trusted parts.
4. Give new expanded authorities to TAPO 2.0 to develop accreditation agreements beyond “five-eyes” to include close partners and allies who are developing new manufacturing capabilities. TAPO 2.0 will also need to develop new accreditation levels and processes for accrediting new microelectronics processing steps, as added authorities may be required.

SUMMARY

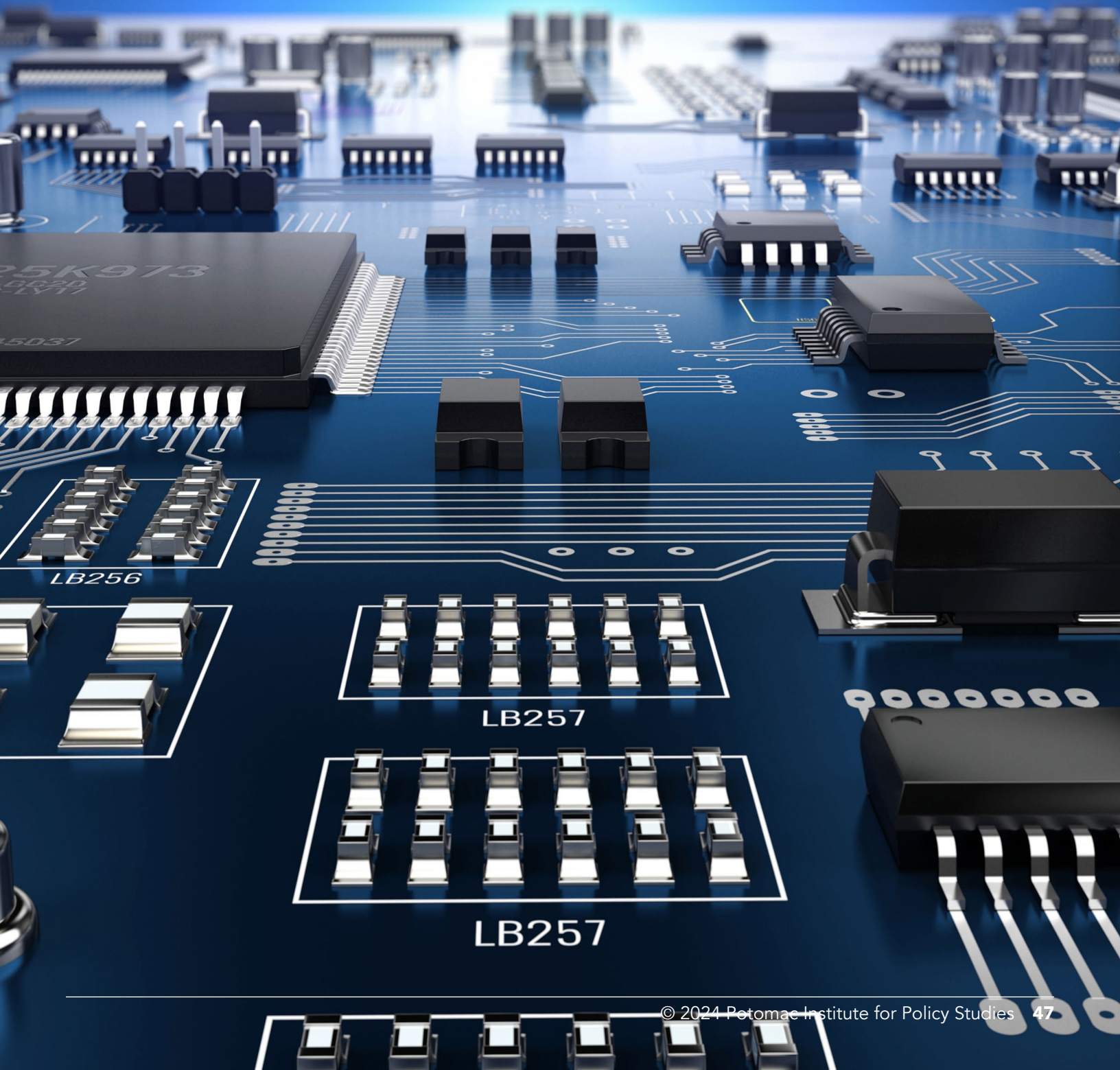
Trust encompasses assured access when both state-of-the-art and legacy parts are needed, and assurance that the parts have high integrity so they can be trusted to perform precisely, as promised, and can satisfy the proprietary and security needs of withholding information from adversaries and competitors. These recommendations are common-sense approaches to completing the mission of the CHIPS and Science Act. With a properly resourced TAPO 2.0, the nation can be assured of an adequate supply of trusted microelectronics to fulfill needs in defense and commercial endeavors that require sufficient trust.

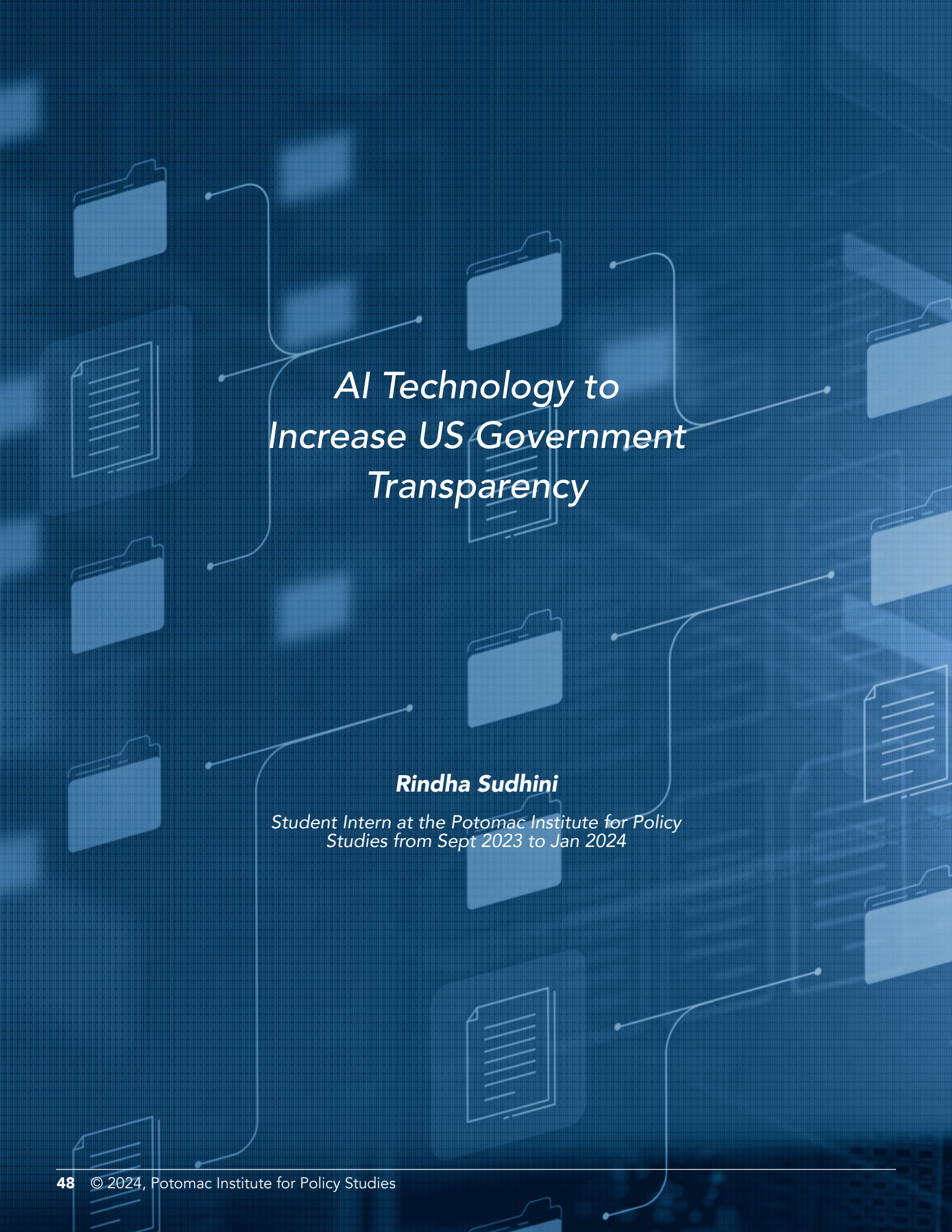
ACKNOWLEDGEMENTS

The author thanks reviewers and contributors Michael Fritze, Daniel Marujo, Bob Hummel, Erica Kilgore and Sherry Loveless for their editorial and contextual support.

ENDNOTES

- 1 Potomac Institute for Policy Studies. (2021). *Re-Embrace American S&T: Reimagine, Reinvent, Restart*. Potomac Institute Press. <https://www.potomac institute.org/steps/featured-articles/september-2021/re-embrace-american-science-and-technology-reimagine-reinvent-restart>
- 2 Office of the Director of National Intelligence. (Feb 6, 2023). *Annual Threat Assessment of the U.S. Intelligence Community*. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>
- 3 NDIA Electronics Division. (2021). *How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base*. National Defense Industrial Association. <https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/ndia-on-shore-semiconductor-products-supply-chain-and-industrial-base-white-paper-final.pdf>
- 4 Potomac Institute for Policy Studies. (2016). *An Analysis of the Impacts of the International Traffic in Arms Regulations (ITAR) on U.S. National Security and Economic Interests*. Potomac Institute Press. <https://potomac institute.org/images/RSEC/ITAR.pdf>
- 5 NDIA Electronics Division. (2021). *How to On-Shore Critical Semiconductor Production, Secure the Supply Chain, and Provide Access for the Industrial Base*. National Defense Industrial Association. <https://www.ndia.org/-/media/sites/ndia/divisions/electronics/images---resources/ndia-on-shore-semiconductor-products-supply-chain-and-industrial-base-white-paper-final.pdf>
- 6 Defense Microelectronics Activity, (2023). *Trusted Foundry Program. Accredited Suppliers*. <https://www.dmea.osd.mil/otherdocs/accreditedsuppliers.pdf>
- 7 US Department of Defense Instruction No. 5200.44. (Nov 5, 2012). *Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)*. <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520044p.pdf>
- 8 Office of the Director of National Intelligence. (Feb 6, 2023). *Annual Threat Assessment of the U.S. Intelligence Community*. <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf>
- 9 Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. (July 2014). *Department of Defense Assured Microelectronics Policy. Senate Report 113-85. DOPSR #14-C-0820*. <https://rt.cto.mil/wp-content/uploads/2019/06/DoD-Assured-Microelectronics-Policy-RTC-July2014.pdf>





AI Technology to Increase US Government Transparency

Rindha Sudhini

*Student Intern at the Potomac Institute for Policy
Studies from Sept 2023 to Jan 2024*



INTRODUCTION

Historically, the federal government has been committed to promoting transparency through information access laws.¹ One such law is the Freedom of Information Act (FOIA),² which allows citizens to request access to records from any federal agency. Even though these requests are meant to be a primary means of providing information to the public, the general citizenry is highly unlikely to attempt to use the FOIA.³ FOIA requests are a notoriously slow process, as most state and federal agencies do not employ digitization or automation techniques in their responses.⁴ Material marked “For Official Use Only” is also not subject to FOIA release. Manually entering requests, logging them through a spreadsheet, and requiring individual judgements are three factors that create an inefficient method of promoting a more accessible government.

Surveys by the Pew Research Center show that many Americans believe that the federal government can and should share more information with the public.⁵ This perceived lack of publicly available information shows that current measures to increase transparency are not working. It also alludes to a growing sense of distrust, as citizens continue to feel distance between themselves and the government. A fundamental psychological construct is that humans tend not to trust what they do not understand.⁶ The extent to which citizens are limited in accessing information about the government, therefore, fosters declining understanding of government proceedings and trust in government.

One possible solution is to employ artificial intelligence (AI) to deal with FOIA requests by facilitating speed and reliability in access and response, and, more broadly, engendering trust in governmental transparency. AI technology can accommodate a considerable volume and range of digital information and can increase the efficiency of government processes. Processes optimized for efficiency and such accessibility promote transparency.

IMPEDIMENTS TO AI-BASED TRANSPARENCY

Using AI technologies to filter and make government data accessible requires increasing digital record-keeping and establishing uniform federal standards of data stewardship. At the same time, users should not employ AI techniques as black-box systems that exclude human-in-the-loop access and that could erode public trust.

Insufficient Digital Record-Keeping

Increased automation in government digitization efforts necessitates increasing digital record-keeping. Many current government processes that deal with official documents and decisions do not use digital forms of the collected data. Reportedly, “only 2 percent of government forms are digitized, 45 percent of websites have not been designed to work on mobile devices, and 60 percent of websites are not fully usable by those who use assistive technologies.”⁷ The government is not leveraging digitization to the extent required to enable AI-based transparency. AI systems require increased access to digital data for more accurate and reliable outcomes.⁸

Inconsistent Federal Data Stewardship Standards

To enable AI systems to access federal digital records, data needs to be organized and structured to facilitate easy access and integration of information. Current standards for federal data stewardship leave much data largely unstructured and disorganized.⁹ Historically, standards were not developed with the intent of using AI systems, but instead were based upon the use of paper archives or, at best, analyses using spreadsheet software. Examples of unstructured data are qualitative statements such as survey responses, social media posts, and voice memos. These represent an untapped information resource with which to enhance government-citizen relations.¹⁰ Structuring data to enable automated ingestion and analysis requires enhanced data stewardship.

Data also need to be securely and equitably organized. Government agencies regularly collect private and sensitive information, requiring robust storage protection measures, such as anonymization, encryption, and other trustworthy access control methods.¹¹ Equity calls for awareness that data collected by the government could have unintentional biases. Data stewardship requires dataset adjustments to correct errors, inconsistencies, and bias to minimize discriminatory outcomes of AI systems. When data are secure and equitable, the resulting outputs will be perceived as more trustworthy.¹²

Trustworthiness of AI

Currently, AI suffers from a “black-box problem”—the dilemma that most AI systems cannot provide an explanation of the reasons for its outputs.¹³ The implications of the black-box problem are significant, particularly when



considering using AI to increase governmental transparency. If the method employed to enhance transparency is inherently opaque and cannot be understood, it may exacerbate the erosion of public trust.

Further, generative AI uses large language models to produce misinformation and “deep fakes.”^{14,15} Unfamiliarity with the power of this technology and its potential risks can also contribute to a lack of public trust.¹⁶ Consumers of AI technology are not typically equipped to discern whether video or audio is original, edited, or generated.

As a result, if AI systems are used to make government actions more transparent, they must be developed and used in ways that anticipate and mitigate public mistrust.

PROPOSED AGENCY RESPONSIBILITIES

To overcome impediments and achieve greater AI-based transparency, the government will have to increase digital record-keeping, establish mandatory standards for federal data stewardship, and mitigate the impact of the “black-box problem.” These issues are difficult to address because no single agency has the expertise and responsibility across all stages of data collection, analysis, and review. In this light, we offer the following proposal to assign specific responsibilities to appropriate agencies.

Digital Data Record-Keeping

While the US government encourages agencies to be more diligent in digital record-keeping (e.g., via the “digital.gov” website in the General Services Administration [GSA]), the focus is not on digitization for AI-type analytics. Legislation, such as Section 508 of the Rehabilitation Act,¹⁷ requires Federal departments and agencies to consider accessibility by those with disabilities. More comprehensive mandatory standards for digital data accessibility and stewardship, with follow-up reporting on compliance (for example, by the GSA), will be needed to increase the availability of digital records for AI-based analytic techniques.

Mandatory Data Stewardship Standards

Currently, federal agencies independently manage their respective data stewardship practices. Lack of guidance and oversight have contributed to vast amounts of unstructured data, which AI systems cannot leverage. The Cybersecurity and Infrastructure Security Agency (CISA) is well-suited to resolve these data stewardship concerns. As an operational component of the Department of Homeland Security (DHS),

CISA is responsible for fostering a secure government technological infrastructure, and already possesses frameworks for collaborating with individual agencies in the cybersecurity space.¹⁸

In 2019, the Office of Management and Budget (OMB) published Memorandum M-19-18, “Federal Data Strategy—A Framework for Consistency” (the FDS),¹⁹ which provides prospective principles and guidelines for agencies to manage and use federal data by 2030. DHS should support CISA with the authority to elaborate the FDS frameworks to incorporate AI technologies. Authorities could be assigned to CISA through legislation, thereby allowing them to establish required standards for organizing unstructured and insecure data.

Congress could also require federal agencies to conduct internal audits to assess the extent to which data stewardship practices comply with CISA standards. CISA would view these audits and engage their oversight authority to draft roll-up reports to update Congress on agencies’ compliance.

Such audits should include internal risk assessments to identify major sources of unstructured and insecure data. CISA could collaborate with agencies to develop specific protocols for structuring and securing new forms of data as they are collected. This approach would allow flexibility in tailoring data stewardship practices to specific data types collected by each agency.

Ensuring compliance with data stewardship standards enhances transparency and public trust by signaling governmental commitment to the responsible use and protection of personal data. CISA should make these standards publicly available, along with their plans for working with individual agencies, to inform citizens how data will be used and strengthen their trust.

Creating a Government AI Training Program

Currently, government AI technology is managed (and understood) by a subset of employees specifically hired for their AI expertise.²⁰ An understanding of data governance and AI technology needs to be consistently distributed across agencies more broadly. The public should not be expected to trust the use of AI systems when many government officials lack a basic understanding of the technologies. To meet this goal, all levels of the government workforce—including leadership—need mandatory training programs that support data and AI literacy.

The General Services Administration (GSA) is an independent government agency established to create an “effective and efficient government for the American people.”²¹ The GSA runs and maintains a technology training interface for all federal employees and, therefore, would be appropriate to oversee AI training programs. “Digital.gov/events” is a GSA training microsite with webinars and events on technology training.

This resource could be expanded to include extensive data governance and AI training programs. Topics should include a basic understanding of standard AI technology (e.g., Natural Language Processing (NLP), computer vision, and generative AI). Trainings should be tailored to: 1) educate employees about the types of AI systems currently employed in the federal government, and 2) provide specialized familiarity with how AI pilot and test cases are employed and operate in their respective agencies. Additionally, current AI regulation and safety practices for AI risk mitigation should be addressed.

Researching Alternative Solutions to the Black-box Problem

Ongoing research in “explainable AI” is proposed to remove the black box problem that contributes, at least in part, to a lack of trust in AI technology.²² As an alternative, AI technology could be configured as a system to cull data rather than make important decisions. Such systems would recognize data that should be identified and parsed for human analysis, thereby ensuring that humans remain in the loop to maintain public trust and ethical standards.²³

The National Institute of Standards and Technology (NIST) has an established network of AI industry partners that can identify technical requirements needed to cultivate safe, secure, and trustworthy AI systems.²⁴ This work qualifies NIST as an appropriate agency to 1) identify technical standards for AI recognition systems that ensure that trustworthy information is provided to human analysts, and 2) research alternative solutions that are developed and implemented to address and reduce the black-box problem.

CONCLUSION

Federal agencies such as the CISA, GSA, and NIST provide ideal environments for overcoming impediments to AI-based government transparency. Employing small groups of specific experts trained to propose standards, create training programs, and research solutions to the black-box

problem greatly increases possibilities for using AI to afford enhanced transparency in government affairs. If successful, such efforts could bolster government-public relations and position the federal government at the forefront of AI integration. In an era of increasing AI prominence, the government must participate in the procedural, policy, and organizational groundwork program developments to regulate the field by setting a responsible precedent and assessing, addressing, and reducing the perceived lack of governmental transparency.

ACKNOWLEDGEMENTS

The author, Rindha Sudhini, performed the work as part of an internship at the Potomac Institute for Policy Studies in the fall of 2023. She wishes to thank the Potomac Institute staff, especially research associate Trevor Huffard, who supervised her internship and assisted in preparing this article.

ENDNOTES

- 1 U.S. Government Accountability Office, *Federal Data Transparency*, Open Data for Accountability, Sep. 30, 2014, <https://www.gao.gov/federal-data-transparency>.
- 2 Freedom of Information Act, United States Department of Justice, <https://www.foia.gov>
- 3 Stephan G. Grimmelikhuijsen and Albert J. Meijer, “Effects of transparency on the perceived trustworthiness of a government organization: Evidence from an online experiment”, *Journal of Public Administration Research and Theory*, vol. 24, no. 1, 2012, pp. 137–157, <https://doi.org/10.1093/jopart/mus048>.
- 4 *FOIA Update: Surrogate FOIA Requests Increasing*, Office of Information Policy, Aug. 14, 2014, www.justice.gov/oip/blog/foia-update-surrogate-foia-requests-increasing.
- 5 *Americans’ struggle with truth, accuracy, and accountability*, Pew Research Center, Washington, D.C., July, 2019, <https://www.pewresearch.org/politics/2019/07/22/americans-struggles-with-truth-accuracy-and-accountability/>
- 6 P.A. Hancock, et al., *How and why humans trust: A meta-analysis and elaborated model*, *Frontiers in Psychology*, Mar. 27, 2023, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10083508/>
- 7 *Why the American People Deserve a Digital Government*, White House Website, Sept. 22, 2023, <https://www.whitehouse.gov/omb/briefing-room/2023/09/22/why-the-american-people-deserve-a-digital-government/>
- 8 Abdulaziz Aldoseri, et al., *Re-Thinking Data Strategy and Integration for Artificial Intelligence: Concepts, Opportunities, and Challenges*, *Applied Sciences*, no. 12, June 13, 2023, <https://www.mdpi.com/2076-3417/13/12/7082>
- 9 *Structured vs. Unstructured Data: What’s the Difference?*, IBM Cloud Education, June 29, 2021, www.ibm.com/blog/structured-vs-unstructured-data/.
- 10 Betsy Gardner, *Unstructured Data: What Is It and Where Do Local Governments Produce It?*, *Data-Smart City Solutions*, Dec. 6, 2021, datasmart.hks.harvard.edu/unstructured-data-what-it-and-where-do-local-governments-produce-it.
- 11 Frank Cremer, et al., *Cyber risk and cybersecurity: a systematic review of data availability*, *Geneva Papers on Risk and Insurance*, Feb. 17, 2022, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/>



- 12 Frank Cremer, et al., *Cyber risk and cybersecurity: a systematic review of data availability*, Geneva Papers on Risk and Insurance, Feb. 17, 2022, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/>
- 13 James S. Denford, et al., *Explainability Won't Save AI*, Brookings, May 20, 2021, www.brookings.edu/articles/explainability-wont-save-ai/
- 14 GAO Science, Technology Assessment, and Analytics, "Science & Tech Spotlight: DEEPFAKES," Feb 2020, GAO-20-379SP, Science & Tech Spotlight: Deepfakes.
- 15 Jiawei Zhou, et al., *Synthetic Lies: Understanding AI-Generated Misinformation and Evaluating Algorithmic and Human Solutions*, Chi '23, Hamburg, Germany, April 23, 2023, <https://dl.acm.org/doi/fullHtml/10.1145/3544548.3581318>
- 16 P.A. Hancock, et al., *How and why humans trust: A meta-analysis and elaborated model*, Frontiers in Psychology, Mar. 27, 2023, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10083508/>
- 17 *Rehabilitation Act of 1973*, U.S. Access Board, <https://www.access-board.gov/about/law/ra.html>
- 18 Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security, <https://www.cisa.gov>
- 19 Federal Data Strategy, Office of Management and Budget, <https://strategy.data.gov/>
- 20 Joseph R. Biden Jr., *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*, The White House, Oct. 30, 2023, <https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>
- 21 U.S. General Services Administration, *Mission and Background*, GSA, www.gsa.gov/about-us/mission-and-background.
- 22 Shaan, *Explainable AI Is Gaining Momentum among VCs and Startups*, Medium, Oct. 24, 2020, [shaan-ai.medium.com/explainable-ai-is-gaining-momentum-among-vcs-and-startups-445906869d01](https://medium.com/explainable-ai-is-gaining-momentum-among-vcs-and-startups-445906869d01).
- 23 Unesco, Conference series "Global Forum on the Ethics of AI," 2024 conference in Feb 5-6, 2024, on "Changing the Landscape of AI Governance." <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>
- 24 *Artificial Intelligence, Overview*, National Institute of Standards and Technology, <https://www.nist.gov/artificial-intelligence>



Featured Authors

Robert (Bob) Hummel, PhD

STEPS, Editor-in-Chief

Chief Scientist, Potomac Institute for Policy Studies

Robert (Bob) Hummel is the Chief Scientist at the Potomac Institute for Policy Studies, the Washington D.C. metro area think tank focused on science and technology issues influenced by affecting national policies. The Institute supports a variety of US government clients, including OSD, NASA, the Air Force, the Space Force, and others.

While at the Potomac Institute, he served on assignment at the National Geospatial-Intelligence Agency. Previously, Dr. Hummel was a program manager at DARPA, managing projects related to automated target recognition, sensor systems, multisensory exploitation, computer science and AI. He is the recipient in 2005 of the Director's Award for Personal Achievement. He worked extensively with DARPA strategy teams, elements of the DoD Joint Staff, and with NGA.

He is a co-founder of the U.S. Technology Leadership Council, a non-profit industry association. Prior to joining DARPA, he was a tenured university professor at the Courant Institute of Mathematical Sciences at New York University. His area of research has been in computer vision and information fusion, with a publication record of articles on object recognition in computer images, image processing, parallel computing, uncertainty reasoning, information fusion, connectionism, and mathematics.

Dr. Robert Hummel has a Ph.D. in mathematics from the University of Minnesota and a bachelor's degree in mathematics from the University of Chicago.



Patrick Ennis, PhD

*Senior Partner, Madrona Venture Group, and Senior Fellow,
Potomac Institute for Policy Studies*



Dr. Patrick Ennis is a Senior Fellow at the Potomac Institute and has spent a career in science, technology commercialization, and venture capital. Patrick is also a Venture Partner at Madrona Venture Group where he helps build startup companies in a wide variety of technologies.

Prior to Madrona, Patrick was at Intellectual Ventures for more than a decade, running startup incubation and technology commercialization with a focus on Asian markets. His investments included Evolv Technology (Nasdaq: EVLV), of which he was a founding board member. Patrick was also the founding CTO of Xinova, a startup that pioneered an international open-innovation market network.

Previously Patrick was a Managing Director of ARCH Venture Partners, where he built early-stage startups for ten years. His investments included Impinj (Nasdaq: PI), Innovalight (acquired by DuPont), and Kotura (acquired by Mellanox/NVIDIA).

Before joining the venture capital industry as a Kauffman Fellow in 1998, Patrick worked at AT&T and Bell Labs, leading projects in software development, speech recognition, and network design. He also worked as a product manager in optical networking and a marketing manager for consumer services.

Before joining Bell Labs, Patrick researched nuclear physics at government labs in North America and Europe. During this time, he published many articles in scientific journals, including *The Physical Review*, *Zeitschrift für Physik*, and *Nuclear Instruments and Methods*.

Patrick has served on the boards of more than 25 private and public companies and educational organizations. In the last two decades, Patrick has spent more than 1,000 days abroad conducting business in 31 countries and developing relationships with technology, corporate, and academic leaders. Patrick holds a Ph.D., MS, and MPhil in physics from Yale, an MBA in finance from Wharton, and a BS in mathematics and physics from William and Mary, where he was elected to Phi Beta Kappa.

Ted Glum

Member of the Board of Directors, Potomac Institute for Policy Studies

Ted J. Glum is a member of the Board of Directors of the Potomac Institute. He is the former Director of the US Defense Microelectronics Activity (DMEA), serving in that capacity from its inception in 1996 to his retirement in 2018. As the Director, Mr. Glum reported to the Assistant Secretary of Defense for Research and Engineering, and was responsible for over \$2 Billion of microelectronics technology programs in addition to numerous classified programs for the Department of Defense (DoD) and Intelligence Community. DMEA capabilities that he oversaw included a one-of-a-kind flexible foundry which enables DMEA to provide critical parts for intelligence, special operations, and combat missions as well as providing parts that are unobtainable in the commercial market, and has been designated as a Critical National Resource by the US Government.



Lisa Hollan

Senior Fellow, Potomac Institute for Policy Studies

Lois Hollan is a Senior Fellow with the Potomac Institute for Policy Studies, and has worked in Washington, DC as a management consultant for US Government Science & Technology programs since 1990. Ms. Hollan has focused on management of complex, high-risk development programs for over 25 years, working largely with the Defense Advanced Research Projects Agency (DARPA). She supported multiple advanced research programs at DARPA and other government agencies in the areas of image understanding, computer vision, automatic target recognition, and airborne video technology communities. Working with the House Science Committee in 2007, she made critical contributions to the legislative drafting and congressional responses related to the Advanced Research Projects Agency – Energy (ARPA-E) bill, leading to passage in 2009. She currently provides management and strategic consulting under the High-Performance Computing Modernization Program to develop rapid simulation technology services in highly complex, physics-based design environments. She has also provided program development support for the National Geospatial-Intelligence Agency Research Division.



In 1983, Lois Hollan was one of the first women in the world to drive a bobsled at the Olympic venue in Lake Placid, NY and became an international leader in the advancing of the sport for women. Those efforts led to worldwide competition and the adoption of the Women's Bobsleigh Olympic event in 2002.

Rindha Sudhini

Student Intern (Sept 2023–Jan 2024), Potomac Institute for Policy Studies

Rindha Sudhini is a rising senior at the University of Pennsylvania where she is majoring in Philosophy, Politics, and Economics with a focus on Public Policy and Governance. In 2023, she completed the Potomac Institute S&T Internship program, where she investigated the relationship between AI/ML applications and civic engagement. Driven by a deep passion for policy, both domestic and foreign, Rindha plans to attend law school after graduation, where she hopes to leverage her understanding of the law to strengthen her advocacy and research efforts.



John Wilson

Senior Fellow, Potomac Institute for Policy Studies

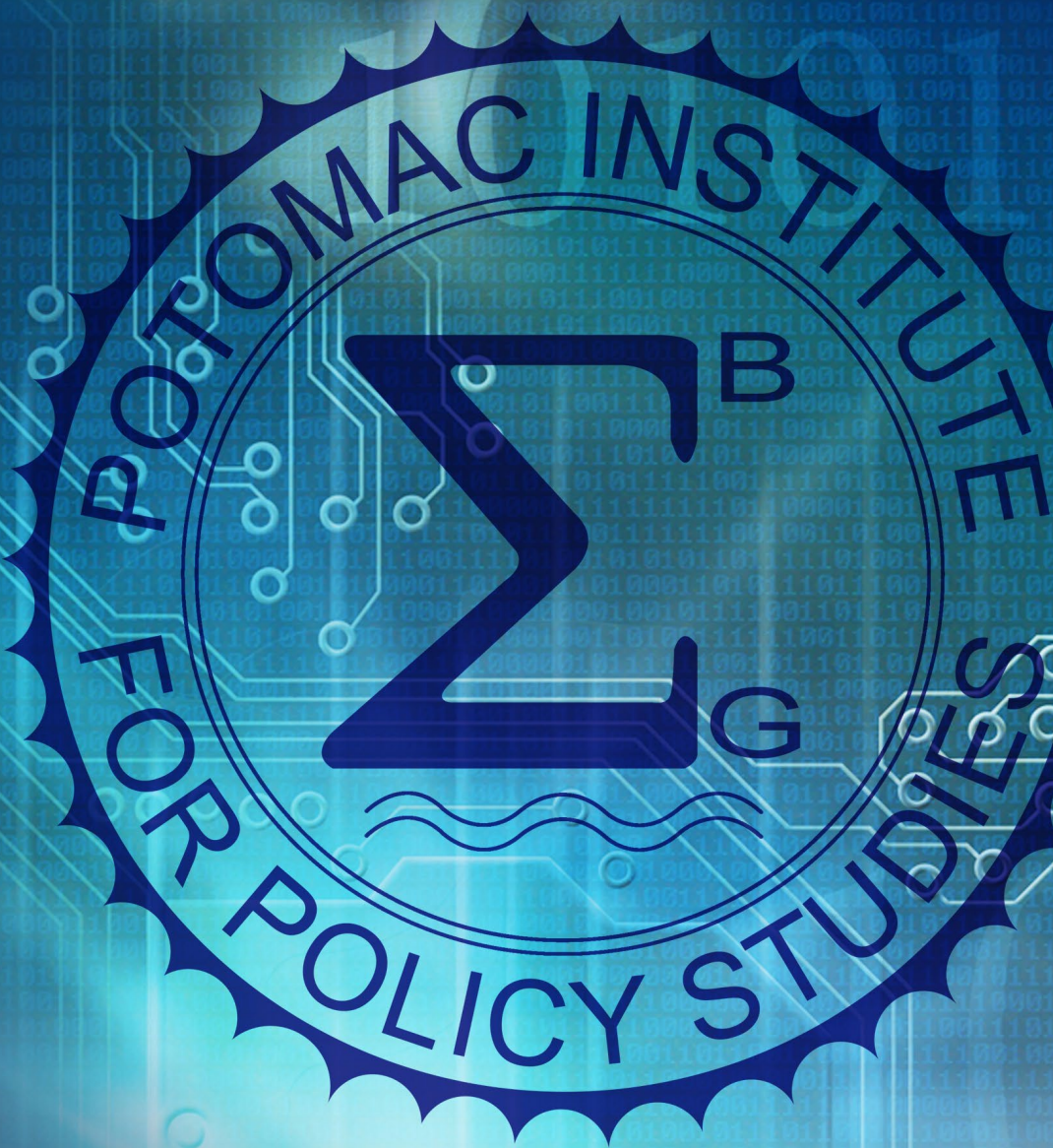
John Wilson is a tech entrepreneur and investor with broad experience across climate tech and innovation structures. For eight years he helped speed US development of electric-drive systems as founding director of a DARPA-funded consortium on transportation advances now known as the Center for Transportation and the Environment. He was CEO of the eMotion Mobility venture with American Le Mans owner Donald Panoz and Daimler that developed an electric Smart car for car-sharing. And he advises Johnson Energy Storage, which aims to commercialize advanced lithium battery technologies invented by former Air Force/NASA rocket scientist Lonnie Johnson.

Early in his career he worked for two members of Congress developing incentives for renewable energy. He then helped expand them as Legislative Coordinator with the Solar Lobby and as founder of the Renewable Energy Institute. Wilson also co-chaired a staff group between Congress and the White House to speed the government's digital transition of legislative and regulatory information. He later founded a Washington office for the Southern Legislative Conference and Southern Governors Association, which he headed for three years.

In 2012 he became a venture partner with Paladin Capital Group, a leading global investor in innovative cyber companies. For four years he was Board Advisor and then Chief Strategy Officer to a publicly traded SaaS delivery management firm. He also cofounded digital display firm NanoLumens and was founding Chairman of social media ratings firm Share Rocket.

In 2011, he helped launch GigTank, a global accelerator for startups on Chattanooga's Gigabit-fiber network. For over a decade he has co-chaired the Technology Association of Georgia's Top-40 innovative firm competition and has served as an investor, mentor or judge with Techstars, Georgia Tech's Flashpoint, NeuroLaunch and CyberLaunch accelerators, Emory University's Excellerator and Valor Venture's Startup Runway. He earned his BA in Chemistry from Emory University.





STEPS (Print)
STEPS (Online)

ISSN 2333-3219
ISSN 2333-3200

