STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 5, 2021

Robert Hummel, PhD
Editor-in-Chief

IN THIS ISSUE

Articles

POTOMAC INSTITUTE PRESS

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, and Editors. The Potomac Institute is non-partisan and does not take part in partisan political agendas.

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

Cover image: "Navigator" by Alex Taliesen.

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@potomacinstitute.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.

Impressum

Editorial and Production Staff

Editor-in-Chief
Robert Hummel, PhD
Email: rhummel@potomacinstitute.org

Associate Editor
Timothy W. Bumpus, PhD
Email: tbumpus@potomacinstitute.org

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

Design + Editorial
Sherry Loveless
Email: sloveless@potomacinstitute.org

About the Potomac Institute for Policy Studies

The Potomac Institute for Policy Studies is an independent, 501(c)(3), not-for-profit public policy research institute. The Institute identifies and aggressively shepherds discussion on key science, technology, and national security issues facing our society. The Institute remains fiercely objective, owning no special allegiance to any single political party or private concern. With over nearly two decades of work on science and technology policy issues, the Potomac Institute has remained a leader in providing meaningful policy options for science and technology, national security, defense initiatives, and S&T forecasting. The Institute hosts centers to study related policy issues through research, discussions, and forums. From these discussions and forums, we develop meaningful policy options and ensure their implementation at the intersection of business and government. A core principle of the Institute is to be a "Think and Do Tank." Rather than just conduct studies that will sit on the shelf, the Institute is committed to implementing solutions.

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

From the CEO

Jennifer Buss, PhD

We live in a world of possibilities wherein science and technology advancements affect our lives every day. However, no advances occur without creative thinking and ingenuity. The Potomac Institute for Policy Studies advocates and encourages new policies and innovations that will change the way we live, work, and learn.

The Potomac Institute for Policy Studies is an independent, nonpartisan, not-for-profit policy research institute. We strive to give you a fair and unbiased look at key science and technology policy issues. Through extensive data collection, research, and analysis, the Potomac Institute provides meaningful policy recommendations and ensures their implementation at the intersection of business and government. We are aware though, that implementation is the most difficult part of policy formation. We aim to be both a think and "do" tank, and the utilization of our work is best shown through the institutions we support. Potomac Institute has conducted hundreds of studies and has provided high-level support to the US Congress, White House, Department of Defense, National Science Foundation, National Aeronautics and Space Administration, Department of Homeland Security, Department of Energy, Intelligence Community, and numerous other organizations.

STEPS: Science, Technology, and Engineering Policy Studies magazine has served as the Potomac Institute's outlet for showcasing forward-thinking researchers, scientists, technologists, and policy makers. *STEPS* authors have argued for an Office of Science policy to streamline science and technology/research and development (S&T/R&D) policy making, suggested acquisitions improvements within government, and discussed ways to navigate the potential pitfalls of S&T policy. While *STEPS* has taken a hiatus, it is important—now more than ever—to hear from those at the top of their fields and to learn what is possible.

With the return of *STEPS* in 2021, the publication will once again be the Potomac Institute's principal venue for highlighting the pressing S&T policy challenges facing us today. We trust that our readers will find the diverse collection of articles informative and insightful, and hope that each issue's contents serves as a useful jumping-off point for public consideration and discourse.

At the Potomac Institute, we pride ourselves on innovative thinking—pushing ourselves and others to see what is possible. Through *STEPS*, we call on bold thinkers and innovators to author articles that make us think, that push boundaries, and that seek to create change. We are excited to relaunch this effort and look forward to what our future *STEPS* authors bring to light. We hope that *STEPS* inspires and initiates change in key science and technology policy issues.

Dr. Jennifer Buss
Chief Executive Officer, Potomac Institute
jbuss@potomacinstitute.org

From the Editor

Robert Hummel, PhD

This issue of *STEPS* inaugurates a new season of articles and notes furthering the mission of the Potomac Institute for Policy Studies. This issue contains a mix of content developed by Institute staff and affiliates and has been heavily influenced by research work conducted at the Institute involving non-attributed experts. Each article presents bold ideas and important discussions—both those impacted by policies and those impacting policies—of topics involving science, technology, and engineering.

With this edition of *STEPS*, we are soliciting articles and notes for future issues. While *STEPS* is an online magazine, it will be broadly distributed and will include articles centralized around the ongoing discussions shepherded by the Potomac Institute through its events and work with the US government and businesses. Articles will be carefully reviewed and edited, and may be submitted by subject matter experts whether affiliated with the Institute or not. Contact me if you have an idea for a future article. I particularly thank my Associate Editor, Dr. Tim Bumpus; the staff of the Institute involved in the production of *STEPS*, including John Mecham and Alex Taliesen; and Sherry Loveless. The next issue of *STEPS* should be available in the late fall of this year!

Dr. Robert (Bob) Hummel
Editor-in-Chief, *STEPS*
Chief Scientist, Potomac Institute
rhummel@potomacinstitute.org

A MICROELECTRONIC “CANARY IN A COAL MINE”

A Call to a New Approach for National Security

Honorable Alan R. Shaffer

Introduction

The United States no longer has the manufacturing capability or access to materials needed for continued economic growth and prosperity for our people. The United States is entering a period of increased national security risk due to lack of access to specific goods and products. One specific industrial sector—microelectronics—is emblematic of the issue. A similar argument could be posed concerning other sectors, like pharmaceuticals and certain raw minerals. But technologies that underpin the development of microelectronics, to include transistors, computers, digital programming, and others,[1] were transformative technologies in which the United States dominated throughout the 20th century. The United States was able to both develop and manufacture products that sprang from them, and to dominate in microelectronics design and manufacture. As the global economy became more entrenched in the 21st century, manufacture and accessibility moved from the United States to other nations. This has led to a situation where both economic and national security is vulnerable due to supply chains that extend to global competitors. Using the semiconductor industry as the example of where supply chains have created vulnerabilities, we call for a new approach to national security by ensuring that critical industries can provide assured access.

This article was originally published online, April 12, 2021.

Background

In the 2020 assessment of the state of the semiconductor industry, the Semiconductor Industry Association (SIA) paints a positive picture,[2] touting that the United States had 47% of the 2019 global market. But the SIA assessment included signs of concern—the year-over-year global market in semiconductors declined from $468B in 2018 to $412B in 2019. Further, Asia accounts for roughly 80% of the physical semiconductor manufacturing. Then came the global COVID pandemic, which highlighted another impact—one that leaves the United States and US allies dependent upon potentially adversarial nations for critical goods. The pandemic highlighted the fragility of the international supply chain and this fragility's impact on national and economic security. For example, given the importance of pharmaceuticals during the pandemic, it became apparent that the United States is dependent on China for over 70% of active pharmaceutical ingredients, according to a *Forbes* magazine article.[3]

In the same article, Kenneth Rapoza quotes members of the Alliance for Manufacturing Foresight (MForsight) stating: "China's 'Made in China 2025' plan, which includes plans to expand in areas such as blockchain technology, artificial intelligence, robotics, semiconductor and chip making technology, along with biotech, *should have the same effect on the US government as Russia sending a man into space* [emphasis added]."[4] COVID only shined a light on practices that were already well underway; China and other Asian countries use subsidies and other incentives to monopolize or dominate a market sector. In so doing, domestic manufacturers (in the United States and other Western nations) become uncompetitive; they transfer manufacturing to Asia or exit the industry all together—to the detriment of US national and economic security. This transfer of domestic manufacturing leaves the United States dependent and vulnerable. The situation is most extreme in the microelectronics industry.

"Designed by Apple in California. Assembled in China."

For the past decade the words embossed on the back of iPhones have served as shorthand for the technological bargain between the world's two biggest economies: America supplies the brains and China the brawn.

"Not anymore. China's world-class tech giants, Alibaba and Tencent, have market values of around $500bn, rivalling Facebook's. China has the largest online-payments market. Its equipment is being exported across the world. It has the fastest supercomputer. It is building the world's most lavish quantum-computing research centre. Its forthcoming satellite-navigation system will compete with America's GPS by 2020."

From* The Economist *"The Battle for Digital Supremacy." March 17, 2018.

Data is the New Oil—The Battle for Digital Supremacy

Microelectronics are the bedrock of the Information Age. Over the past several years, futurists have been using the phrase "data is the new oil" when talking about the foundation of the global economy.[5] Just as oil drove the Industrial Era, data is driving the Information Era. The Information Era touches all walks of life from the consumer to the warfighter, and national and economic infrastructure. From a systems engineering viewpoint, one collects the raw information (sensors), stores the data (memory), transports the data (communications), and processes the data (as in artificial intelligence). Then, the result is displayed for action or insight. Each of these phases is wholly dependent on microelectronics. To be competitive in the information age, one must have access to a plethora of diverse microelectronics.[6] Literally, the world has entered into the era of the “Battle for Digital Supremacy,” according to the title of an *Economist* article.[7] The article begins by making the case that China’s information technology companies have evolved from manufacturing designs made by more technologically advanced nations (primarily the United States) to the present where Chinese companies have achieved technological parity or beyond with the West (United States and Europe).

If data is the new oil, digital supremacy is the foundation—the nation or coalition that can better navigate the world of data will have dramatic advantage in the consumer, military, national and economic security, and political spheres, which are the main components of national power.

Evolution of Microelectronics Manufacturing—United States in Decline

From the earliest days of the microelectronics industry, the United States has been the global semiconductor leader, consistently accounting for 45% to 50% of global sales (i.e., purchases of microelectronics); even today, the market share of sales is 47%. The spinoffs out of Fairchild Semiconductor in the 1960s spawned the world’s microelectronics industry, which created market-leading companies to include Intel, AMD, Sun, CISCO, NVIDIA, and others. But now, reportedly, the US share of the global semiconductor *manufacturing* capacity has fallen to 12% from 37% in 1990, and is expected to fall further as only 6% of the new global capacity is projected to be located in the United States.[8] A February 2021 letter from 21 semiconductor industry CEOs to the President, citing these statistics, called for semiconductor manufacturing incentives and for research grants.[9]

These same data project that without such incentives, the combination of China, South Korea, Japan, and Taiwan will exceed 80% of the world manufacture market by 2030. Moreover, they project that the compound average growth rate for microelectronics manufacture in the United States is roughly half of the rest of the world combined—the US industrial manufacturing capacity will rapidly diminish to a small fraction of the rest of the world.

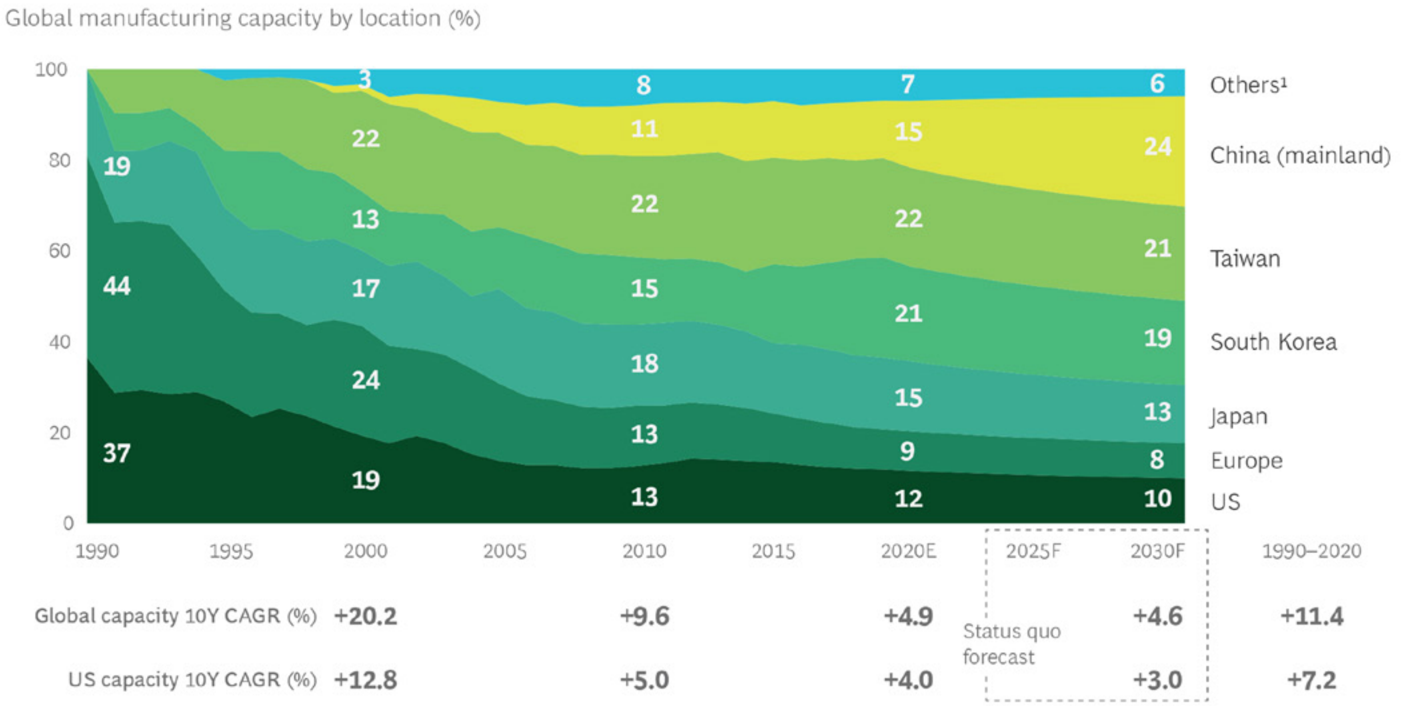
We, thus, present the following three findings, which leads to a serious conclusion for US national and economic security:

- The US market demand for finished microelectronics products remains strong, at roughly half of the world market.
- Over the last 30 years, the US manufacturing volume has declined to about 10% of global share, compared to 50% in Taiwan and China.
- Manufacturing growth in Asia (and the rest of the world) is twice that of the United States (and Europe).

Therefore, an economic engine in microelectronics in the United States is built on a supply chain that may or may not be available to the United States, and the situation is becoming more extreme. As we will see, this dynamic may have affected the US economy in 2021.

To emphasize the finding that the United States is being phased out as a producer of microelectronics—detrimental to US access to these parts—please see Figure 1, which is based on projections from VLSI Research of global semiconductor manufacturing capacity.

There are several sectors of the domestic (US) microelectronics industry where there is even less capacity—notably memory, integrated circuits, and packaging and test facilities (which are called the Out-Sourced Test and Assembly, or OSAT, sector). The United States retains about 85% of the electronic design automation (EDA) tools sector, but only has 12% of the logic and 4% of the memory manufacturing markets.[10] The OSAT sector is already controlled by China and Taiwan, with less than 5% of the market in the United States.[11] The OSAT global market in 2018 was reportedly $27.7B, with all but one of the top ten OSAT companies (by volume) headquartered in Taiwan, China, and Singapore. Even when companies have offices or headquarters in the United States, manufacturing factories are mostly located overseas. Trade associations collect and sell detailed information concerning market sizes and the sales volume of OSAT firms worldwide,[12] documenting the outsourcing of packaging and testing of semiconductors to a relatively few foreign facilities.



Sources: VLSI Research projection; SEMI second-quarter 2020 update; BCG analysis.

Note: All values shown in 8" equivalents; excludes capacity below 5 kwpm or less than 8".

¹ Includes Israel, Singapore, and the rest of the world.

Figure 1. Growth in the US Installed Capacity has been Outpaced by Asian Countries. Reproduced with permission from the Boston Consulting Group (BCG).[13]

Said simply, the United States still has a dominant position in EDA tools for circuit design, but then sends the design to a non-US company to take the design to physical capability. What is less understood is that manufacturing processes and designs are just as critical, if not more, to producing highly complex circuits. The United States is no longer driving production and has become reliant on other nations.

Loss of Manufacture and Protection of Intellectual Property

Why does the fact that both manufacturing and package and test are conducted offshore present a challenge? Many would argue that this is just part of the global nature of the business. The issue is a loss of intellectual property (IP), which in turn, erodes the leading nation's advantage.

We noted that the United States still is dominant in design of high-end microelectronic systems and applications. Unfortunately, the US-led design is outsourced for semiconductor manufacturing and for package and test. When designs are shared with manufacturers and packaging companies, they become much more vulnerable to IP theft. According to a 2019 article in *Fortune Magazine*, one in five US companies allege that they were a victim of IP theft within the past year, and a 2018 US Trade Representative report cited the estimated theft of US IP by China at $250-600B per year.[14]

In a 2017 article in *The Economist* magazine, the authors wrote: "think of Chinese competition as having three dimensions: illegal, intense, and unfair."[15] China and other countries have shown a propensity to engage in IP theft (the "illegal"), at enormous scale (the "intense"), leading to a situation whereby the theft of IP leads to a reduction in overhead cost that provides an advantage (the "unfair"). Where this becomes critical is in the outsourcing of the microelectronics manufacture and packaging and test, which permits China—or any other nation that would choose to engage in IP theft—to do so, and thus, reveal the design of the devices. The export of US microelectronic designs is a challenge to US national security. The current structure will lead to a loss of US advantage in short order.

While it appears that there may be some movement to diminish theft, it is clear from China's 14th five-year plan that the People's Republic is investing heavily in microelectronics, to include design.[16] This five-year plan specifically discusses major Chinese investment in microelectronics research and development centers in other countries. We believe this indicates continued willingness to advance China's design capabilities by any means possible.

Continuation of outsourcing of package and test to Asia makes the Chinese job to advance indigenous design easier. In other domains, China has clearly used predatory business practices to bridge the innovation gap,[17] and the outsourcing of package and test makes this practice in the microelectronics domain much easier. In essence, the outsourcing of package and test risks relinquishing the US advantage in design. And when design goes offshore, so does manufacturing, thereby directly impacting US national security.

Furthermore, outsourcing of package and test questions the assurance and security of these parts. It is far too easy to substitute counterfeit parts. This endangers critical national security systems and consumer electronics, as well.

The Canary in the Coal Mine—Global Shortage of Specific Microelectronics

The COVID pandemic has reduced the worldwide demand for certain specialized chips (microcontrollers) needed for automobiles, while the "work at home nature" expanded the need for higher end communications and computer chips, as detailed in a *Washington Post* article.[18] Production shifts were made by industrial partners in Asia, who did not take into account potential North American and European markets. As the world worked through the change in demand for specific chips, the microelectronics providers shifted focus from specialized automotive microcontrollers. This supply chain disruption is leading to a contraction in the number of new vehicles in 2021 by 1.5 to 5 million automobiles (from a base production in North America and Europe of 20 million units in 2019). The estimated cost to the global economy in 2021 is in excess of $60B.[19] The *Washington Post* article cited Tom Caulfield, CEO of GlobalFoundaries as saying "Ford, Volkswagen, BMW, Daimler-Benz, Fiat, Chrysler, GM….every one of them became my new best friend."[20] Of note, this shortage has not been reported by Hyundai, Kia, and other Asian auto manufacturers.[21] It is also interesting to note that 70% of the specialized microcontroller chips come from TSMC, in Taiwan. As the post-event analysis is done, it will be important to verify if the supply chain disruption occurred only in the West.

While this event may represent an unfortunate convergence of events, it should be seen as the "canary in the coal mine event" of the vulnerability of the West to a single-source, non-assured supply. This incident may well be the early signal or wake up call to a more serious problem for the United States.

Lack of domestic microelectronics production is a problem in both national and economic security, for both government and commercial sectors. As the United States exits the manufacturing sector, it will not return soon, as a new microelectronics fabrication facility costs anywhere from $4B to $20B for a state-of-the-art facility (depending upon function). Further, it takes four or more years to begin production. For example, in 2020, TSMC proposed building a new $12B fabrication facility in Arizona.[22] Because of the specialized nature of semiconductors, and the cost involved with changing process lines, any disruption to the supply chain could and will ripple through the industry.

Breadth of the Microelectronics Challenge—It is Not Just Package and Test

The 2021 shortage of microcontroller chips is currently the most visible manifestation of security challenges for the United States in the microelectronics world. However, this supply chain disruption did not occur as a result of outsourced package and test, but rather due to specialized logic chips largely manufactured by TSMC. We noted earlier that over 95% of package and test capacity resides in Asia. We also know that roughly 80% of all memory devices come from foundries in Korea, Japan, and Singapore.[23] In fact, the current automotive shortfall is in a sector where US manufacture capacity is actually better relative to memory and package and test. Therefore, we could expect similar or worse outcomes if we lost assured access to other microelectronics components where the United States no longer has a substantial market share, such as memory.

National Security Challenges Due to Economic Actions

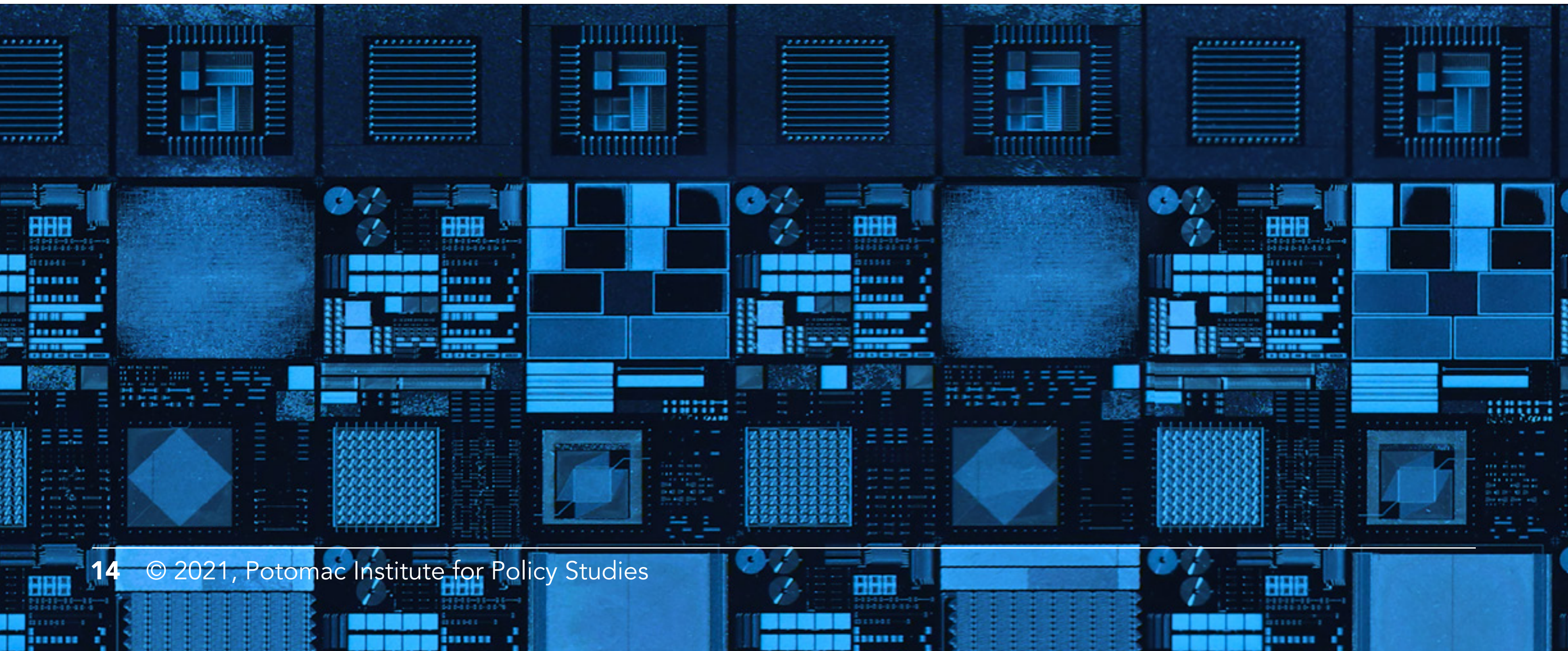
So, what is the "concern"? What if a country decides to use the relative imbalance in production capacity with the United States as a political or economic lever?

This has been done before; and the analogy is ironic. The underlying foundation of the Industrial Era was oil. In 1973, the Organization of the Petroleum Exporting Countries (OPEC) ministers decided to restrict the production and distribution of oil to the West. At the time, the United States did not produce as much oil as it consumed. In 1973, the United States consumed 17.3M barrels per day (bpd), but only produced 11.4M bpd, so the imports of 6.26M bpd accounted for 36% of the US consumption.[24] When coupled with other effects, like the decoupling of oil and gold (the end of the Bretton Woods agreement) and the US support for Israel in the Arab-Israeli war, the OPEC states restricted exports to the United States and other net importing nations. The result of the oil crisis was a four-fold increase in the cost of oil and the recession of 1973-1975. Coming out of this shock was hard; the US economy suffered from "stagflation" and a weakened economy.

While this example is a simplification, during the 1973 oil crisis, a small group of nations successfully controlled access to the underlying economic foundation. This resulted in an overamplified response in the West (to include North America). The same political or economic levers could be used on the United States or its allies with the microelectronics industry if the United States and US allies don't revitalize the ability to meet manufactured demand. Actually, the impact could be much worse than during the 1973 oil crisis. OPEC is comprised of 13 member nations that control 44% of the global oil production and about 80% of the known reserves; in the 1970s, the United States depended on imports for only 36% of their energy needs. A microelectronics analogue to OPEC comprised of China, Taiwan, and South Korea would account for much more that 44% of the global microelectronics production, and the United States is importing as much as 80% of the microelectronics for US domestic use. The current demographic shift in microelectronic manufacture capability leaves the United States extremely vulnerable economically.

Simply stated, US and Western manufacture capacity currently does not meet the demand for microelectronics. If a country needs something that they do not produce, there is an inherent vulnerability. The United States is vulnerable. In microelectronics, this vulnerability is getting more acute, especially for national security. Further, the future economic structure of the United States is dependent on a supply of microelectronics outside of US control, which further jeopardizes future access to state-of-the-art technological capabilities. As seen with the "canary in the coal mine" example of microelectronics and the automobile industry, modern systems rely on access to the supply components not made domestically.

Congress has taken note of this problem. A February 2021 report "Beat China: Targeted Decoupling and the Economic Long War" released by Senator Tom Cotton (R-AR), points out that subsidy (government incentives) provided to the microelectronics industry by the US and Western European nations is roughly one-half to one-third that of South Korea, Taiwan, Singapore and China.[25] Senator Schumer (D-NY) has called on fellow lawmakers to craft a package of measures that "target investment in US manufacturing, science and technology, supply chains and semiconductors…to counter China's rise…to strengthen the US tech sector,



and [to] counter unfair practices."[26] Senator Mark Warner (D-VA) is the lead co-sponsor of the Democracy Technology Leadership Act, which states "The People's Republic of China is pursuing a set of policies to achieve dominance in key technologies…" and calls on an international partnership to counter China's practices.[27] In an interview, Senator Warner stated, "This is the defining economic issue of our time, there needs to be a sense of urgency… ."[28] On February 24, 2021, an Executive Order on "Securing America's Critical Supply Chains" explicitly directed a 100-day review of vulnerabilities caused by supply chain weakness in four specific industries: 1) active pharmaceutical ingredients; 2) critical minerals; 3) large capacity batteries; and 4) semiconductors and advanced packaging.

The challenge to the United States is becoming clearer with every passing day. From the initial shift of manufacture to Asia through the current "canary in the coal mine" event, the challenge is seen as largely apolitical—continuation of American economic, political, and national security strength has a foundation in microelectronics—and needs to be addressed today.

A Path Forward?

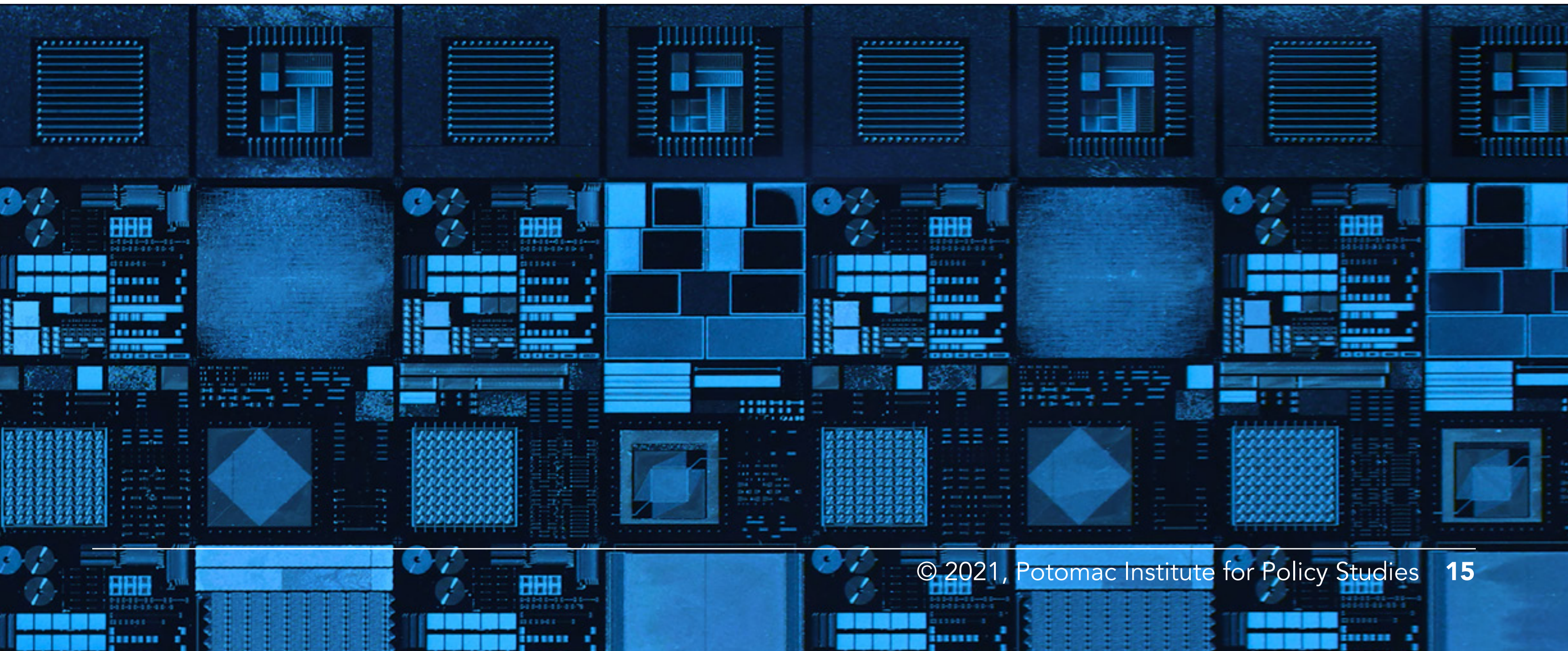
We have seen that there are national and economic security vulnerabilities with respect to microelectronics. The current economic playing field is not level—other countries, primarily in Asia, heavily incentivize their industries, and force in-country manufacturing as a means of market addressability leading to an unequal market balance.[29] Without addressing the economic competitiveness of the US microelectronics industry, a sustainable business model will be challenging. It is, nonetheless, achievable.

This problem cannot be solved by either government or industry alone. The solution must resolve the cost differential between Asian firms and US-based companies. Discussions with US-based microelectronics industry executives indicate they can be competitive if the underlying cost structure is within 10% equivalency as opposed to the current 20-30% difference.[30] This paper will not explore solutions deeply but will suggest some ideas that will need further elaboration.

The key point is that the scale and complexity of the problem requires new vectors of attack, and likely a public-private partnership for economic incentives coupled with a regulatory approach that restricts application of microelectronics from certain non-allied sources. Standard government approaches have not worked in the past; new and more innovative approaches are likely required.

Policy Options

A Berry Amendment-like statute: USC 10 Section 2553a is the law known as the Berry Amendment—a statute that requires the Department of Defense to buy certain goods from domestic sources. Effectively, the Department of Defense must buy clothing, food, and some specialty metals from domestic sources. Development of a similar policy to direct microelectronics used for national security to be "Made in America" would provide incentives for domestic industry. Note that this restriction would not be limited to the Department of Defense (DoD), but rather, would cover all



national security systems. In the past, when people thought about directing vendors to use pedigree microelectronics for national security systems, the proposers typically limited themselves to defense systems. Defense systems comprise about 2% of the total domestic market, and thus don't drive production. In the information world, national security and economic imperatives include the military and sectors of critical national infrastructure, such as electric grids, sensitive verticals (banking, medical, etc.), transportation, and the national communications grid. Including all of these sectors grows the demand to nearly 25% of the United States market for microelectronics and is large enough to make a difference, affording a sizable and sustainable business model.

Enhanced Import Tariffs on Subsidized Goods: As discussed, most Asian nations subsidize their industry to enhance the Asian vendor competitive posture. While not illegal, it is not a practice available to domestic providers, nor is it "fair." Increasing tariffs on imported chips could level the playing field. There are potential hazards to overall US competitiveness, but these risks are costs for security. While this does not, in and of itself, solve the problem of assured and secure pedigree of parts, it would provide a more level playing field for domestic producers.

Financial Options

Direct Company Subsidy: This option would be a direct investment by the US government into vital companies that are the most difficult to replicate. This could be done by either a standard competitive "FAR" (Federal Acquisition Regulation)-based solicitation or via a grant through something like the Defense Production Act. The previously cited publication by the BCG and the SIA predicts that the US market share will decline to 10% by 2030, despite building 9 new fabs.[31] A $20B investment would increase the fabs and market to 14 and 12%, while a $50B investment would result in 19 new fabs and 14% of the global market. More importantly, the investment could enhance the United States as a state-of-the-art provider. Unfortunately, the model presented here has been tried before, and would likely require continued investment because it does not solve the issue of volume and continued viability of the partner who receives the grant. In the past, the DoD was never able to increase purchase volumes to make the investment sustaining. Whatever is done, there will need to be both financial and policy incentives.

A mix of investment and loans: Suppose that, instead of a direct procurement, the government entered as a partner with industry. This is a more radical thought, because it uses government capital executed through an industrial company. As a partner, the US government may invest using a combination of direct investment and government-backed loans, such as are available from the Export-Import Bank (EXIM) or some other entity. In addition, the government can include procurements of capital equipment which can be "loaned" to industry and written off. There are also options with long-term commitments and regulatory support. Several ongoing studies are in the process of evaluating additional financial models that focus on potential solutions to either the Administration's Build Back Better Plan or the Congressional CHIPS for America Act[32] to enhance large-scale domestic production, with the idea of incentivizing private capital to co-invest.

Summary

As the world has moved into the era of data and information technology, data has become the new oil. Data systems and data processing are the key drivers of economic growth and national security and rely heavily on modern microelectronics. Without a secure and stable microelectronics supply, both economic stability and national security are vulnerable.

Currently, sources of microelectronics and their manufacture are concentrated in Asia, and in particular in China, which has caused the United States and many allied nations to become reliant on limited or non-reliable sources. This dependence has been increasing.

The causes of the concentration are myriad, but we have argued that deliberate unfair policies underlie the resultant dependence on China and certain Asian countries. These causes include the use of intelligence services to access Western IP at a massive scale, and heavy government subsidies to support industries in the microelectronics sector. China, in particular, continues to exercise predatory business practices that put the US posture in microelectronics at risk.

The vulnerabilities include the potential loss of access, at any time, whether deliberate or as a consequence of geopolitical events, which can harm economic interests or damage national security. As dependence increases, the United States becomes ever more vulnerable politically, economically, and militarily. This is a serious national security issue.

Solution to the challenge will not be found in either classic economic or government actions. Both policy and financial factors could mitigate the national security challenge, but addressing this will take a multi-prong approach involving government, industry, and academia, with regulations and incentives that over time will diminish US dependence. Congress and the Administration have taken note of the issue and have responded with multiple proposals attempting to strengthen the US microelectronics manufacturing capacity and promote innovation.

However, the nation must respond strategically. The United States did not get in this position quickly and getting out will take time, focused investment, and careful policy considerations. Microelectronics is but one sector—albeit critical—in which vulnerabilities must be reduced. A strategic plan to reassert US leadership in microelectronics, and success in this critical endeavor, would serve as a model across all sectors of critical importance to US economic and national security. It is now time to act on this strategic issue.

Endnotes

[1] Durius Stusowski, “These Five Technologies Dramatically Changed the 20th Century,” March 14, 2017, https://historycollection.com/5-impactful-technologies-20th-century/3/.

[2] “2020 State of the Semiconductor Industry Annual Report,” Semiconductor Industry Association, https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf.

[3] Kenneth Rapoza, “Why is the United States so Ridiculously Dependent on China,” *Forbes* April 30, 2020, https://www.forbes.com/sites/kenrapoza/2020/04/30/why-is-the-us-is-so-ridiculously-dependent-on-china/?sh=e8c059e56b5c.

[4] Kenneth Rapoza, “Why is the United States so Ridiculously Dependent,” referring to: Sridhar Kota and Thomas C. Mahoney, “Invent Here, Manufacture There,” *Insight into Manufacturing Policy* 20 (March) 2020, http://industrialpolicy.us/resources/Manufacturing/LossOfProductionCapabilities.pdf.

[5] Mathematician Clive Humby is credited with coining the phrase; Others using the phrase include UnderArmor CEO Kevin Plank, and Director Emeritus of University of Southern California Innovation Lab Jonathon Taplin.

[6] Throughout this paper, I am using the generic term “microelectronics” to include integrated circuits (logic devices, mixed signal chips), memory, and others.

[7] “The Battle for Digital Supremacy,” *The Economist Magazine* March 17, 2018.

[8] Antonio Varas, et al., “Government Incentives and US Competitiveness in Semiconductor Manufacturing”, Boston Consulting Group and the Semiconductor Industry Association, Sept 2020, https://www.bcg.com/en-us/publications/2020/incentives-and-competitiveness-in-semiconductor-manufacturing.

[9] Semiconductor Industry Association (SIA), SIA Board of Directors, letter to the President dated Feb 11, 2021. https://www.semiconductors.org/wp-content/uploads/2021/02/SIA-Letter-to-Pres-Biden-re-CHIPS-Act-Funding.pdf.

[10] Antonio Varas, et al., “Government Incentives and US Competitiveness.”

[11] Antonio Varas, et al., “Government Incentives and US Competitiveness.”

[12] Antonio Varas, et al., “Government Incentives and US Competitiveness.”

[13] Market Research Reports, “Global 3D Semiconductor Packaging Market Growth (Status and Outlook) 2021-2026,” https://www.marketresearchreports.com/lpi/global-3d-semiconductor-packaging-market-growth-status-and-outlook-2021-2026.

[14] Eric Sherman, “One in Five US Companies Say China Has Stolen Their Intellectual Property,” *Fortune* March 1, 2019.

[15] “How China is Battling Ever More Intensely in Global Markets,” *The Economist* Sept 23, 2017.

[16] Congressional Research Service summary, “China’s 14th Five Year Plan: A First Look, January 5, 2021.

[17] Yukon Huang and Jeffery Smith, “China’s Record on Intellectual Property Rights is Getting Better and Better,” *Foreign Policy* Oct 16, 2019.

[18] Jeanne Whalen, et al., “No Quick Fix for Chip Shortage, Hobbling Factories,” *Washington Post* March 2, 2021: A1.

[19] Michael Wayland, How Covid led to a $60 Billion Global Chip Shortage for Automakers, *CNBC* Feb 11, 2021, https://www.cnbc.com/2021/02/11/how-covid-led-to-a-60-billion-global-chip-shortage-for-automakers.html.

[20] Jeanne Whalen, et al., “No Quick Fix.”

[21] Joyce Lee, “Analysis: Hyundai Bought Chips When Rivals Didn’t, Its Assembly Lines are Still Rolling,” *Reuters* Feb 26, 2021, https://www.reuters.com/article/us-autos-semiconductors-hyundai-motor-an/analysis-hyundai-bought-chips-when-rivals-didnt-its-assembly-lines-are-still-rolling-idUSKBN2AQ0EF.

[22] Sharisse Pham, “Taiwan Chip Maker TSMC’s $12 Billion Arizona Factory Could Give the US an Edge in Manufacturing, *CNN Business* May 15, 2020, https://www.cnn.com/2020/05/15/tech/tsmc-arizona-chip-factory-intl-hnk/index.html.

[23] 2020 State of the US Semiconductor Industry from the Semiconductor Industry Association, https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf.

[24] US Energy Information Agency (www.eia.gov).

[25] Antonio Varas, et al., “Government Incentives and US Competitiveness.”

[26] Richard Cowan and Alexandra Alpers, “Top US Senate Democrat directs lawmakers to craft bill to counter China,” *Reuters*, February 21, 2021, https://www.reuters.com/article/us-usa-china-democrats/top-u-s-senate-democrat-directs-lawmakers-to-craft-bill-to-counter-china-idUSKBN2AN2HJ.

[27] Mark Warner, “Bipartisan National Security Leaders Agree: ‘The Democracy Technology Partnership Act Outlines an Important Vision and Strategic Plan for the U.S.’,” Mar 30 2021, https://www.warner.senate.gov/public/index.cfm/press-releases?ID=AE800673-B962-4F48-AC10-F203760D2F74.

[28] Mark Scott “Senior US Senator Calls for Western Tech Alliance Against China,” *Politico*, 12 March 2021, https://www.politico.eu/article/mark-warner-digital-bridge-tech-china/.

[29] There is also a fairly substantial body of evidence that China deploys their nation-state intelligence services against companies competitive with their state-owned enterprises.

[30] Private discussions between the author and select microelectronics CEOs/COO. Also, the 30% difference is explained in Antonio Varas, et al., “Government Incentives and US Competitiveness,” Exhibit 8.

[31] Antonio Varas, et al., “Government Incentives and US Competitiveness.”

[32] H.R.7178 - 116th Congress (2019-2020): CHIPS for America Act | Congress.gov | Library of Congress, https://www.congress.gov/bill/116th-congress/house-bill/7178.

SECURING
Critical Supply Chains

Michael S. Swetnam[†] *and Jennifer Buss, PhD*

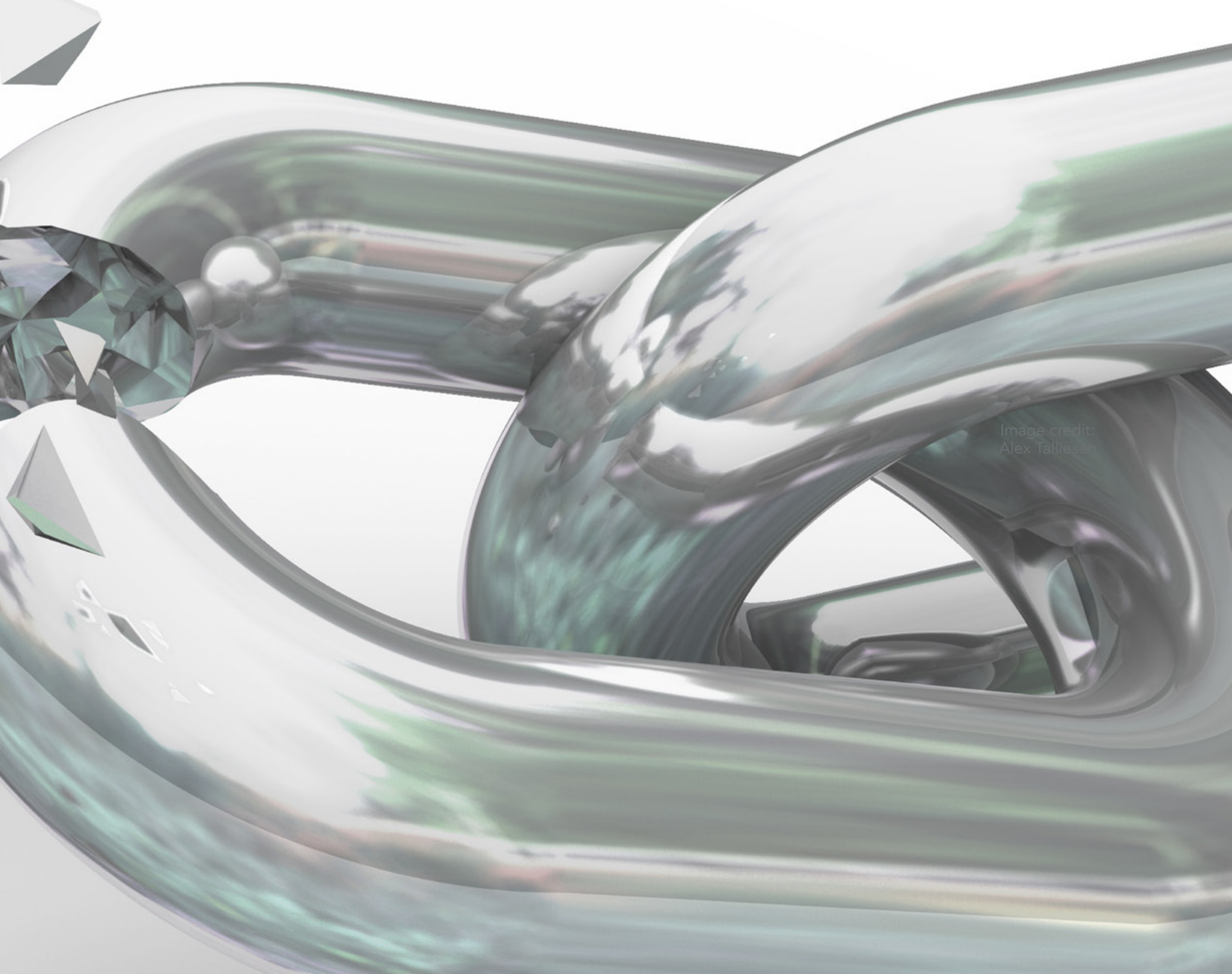


Image credit:
Alex Talliesen.

[†] Deceased.

Strategies for Sovereignty Over Critical Supplies

During times of crisis, such as the COVID-19 pandemic, the significance of securing critical supply chains to uphold national security becomes evident. How can the United States maintain sovereignty and protect its interests when our economy and national security are dependent on external, global supplies of services and products?

We discuss three strategies that the United States can adopt to maintain full sovereignty over critical supply chains:

1. Fully US Controlled Critical Supply Chain
2. MAD-1: Mutually Assured Dependence
3. MAD-2: Mutually Assured Destruction

Full Control

The first strategy for maintaining sovereignty is a fully US controlled critical supply chain. If the United States controls its own critical manufacturing capabilities, then foreign countries cannot threaten leveraging necessities against the United States, nor will they be able to withhold necessities to meet their own demand. This strategy demands national acquisition by any means to own, control, and access all critical services and materials necessary for the full functioning of our economy and security. For example, for our nuclear stockpile, the United States requires full control of all aspects of production and maintenance. Full control usually entails domestic production, but might include alternative sources in which full control is assured.

While this is the most secure strategy, it is also arguably the least stable and most problematic. As technology has become increasingly complex, manufacturers have turned to specialists and subcontractors to narrowly focus on just one area of expertise. This has created a deep tiering of supply chains, where each tier is dependent on the one below it. Visibility into more distant tiers is challenging, making wholesale replacement of supplies at any link in the chain very difficult. Moreover, modern manufacturing of products requires a highly skilled and trained workforce, which the United States lacks in certain critical areas, because operations management has turned into procurement leadership. The job of taking a product into manufacturing has increasingly turned into one of offshore product sourcing.

A fully controlled US critical supply chain is a potentially attainable goal, and provides the greatest security, but it would require immense investment and effort, and risks isolationism.

MAD-1

The next strategy for maintaining US sovereignty is a plan of mutually assured dependence (MAD-1). Under this strategy, the United States would only allow dependence on another country's critical resources and services if we have commensurate leverage against that country. Within this scenario, the United States would be able to deny a foreign entity access to as critical a set of resources and services as they can deny us.

This strategy is arguably the easiest to implement but is one of the least secure. It is very difficult to achieve a balance of equally weighted dependence, especially because from day to day and month to month, the level of importance of critical recourses and services changes. For example, the day-to-day importance of N-95 masks was perceived as lower before COVID-19 than at the height of the pandemic. During other types of crises, wars, or economic downturns, different critical goods become more of a necessity than others. If a foreign entity decides that it is worth it for them to cut the United States off from critical services and resources, despite the losses they will face, then the United States will be left extraordinarily vulnerable. If a country reneged, the only two options would be to accept the reduction in capability, or shift to the next strategy (MAD-2).

MAD-2

The final strategy is a plan of mutually assured destruction (MAD-2). Under this strategy, the United States maintains a large enough and superior enough military force to seriously demand access under threat of war in the event of some foreign entity's wish to deny US access to critical services and resources. The original MAD concept is that each side could assure annihilation of the other side. This version contemplates an overmatch capability, wherein one side can threaten the other side sufficiently enough to deter supply chain disruptions.

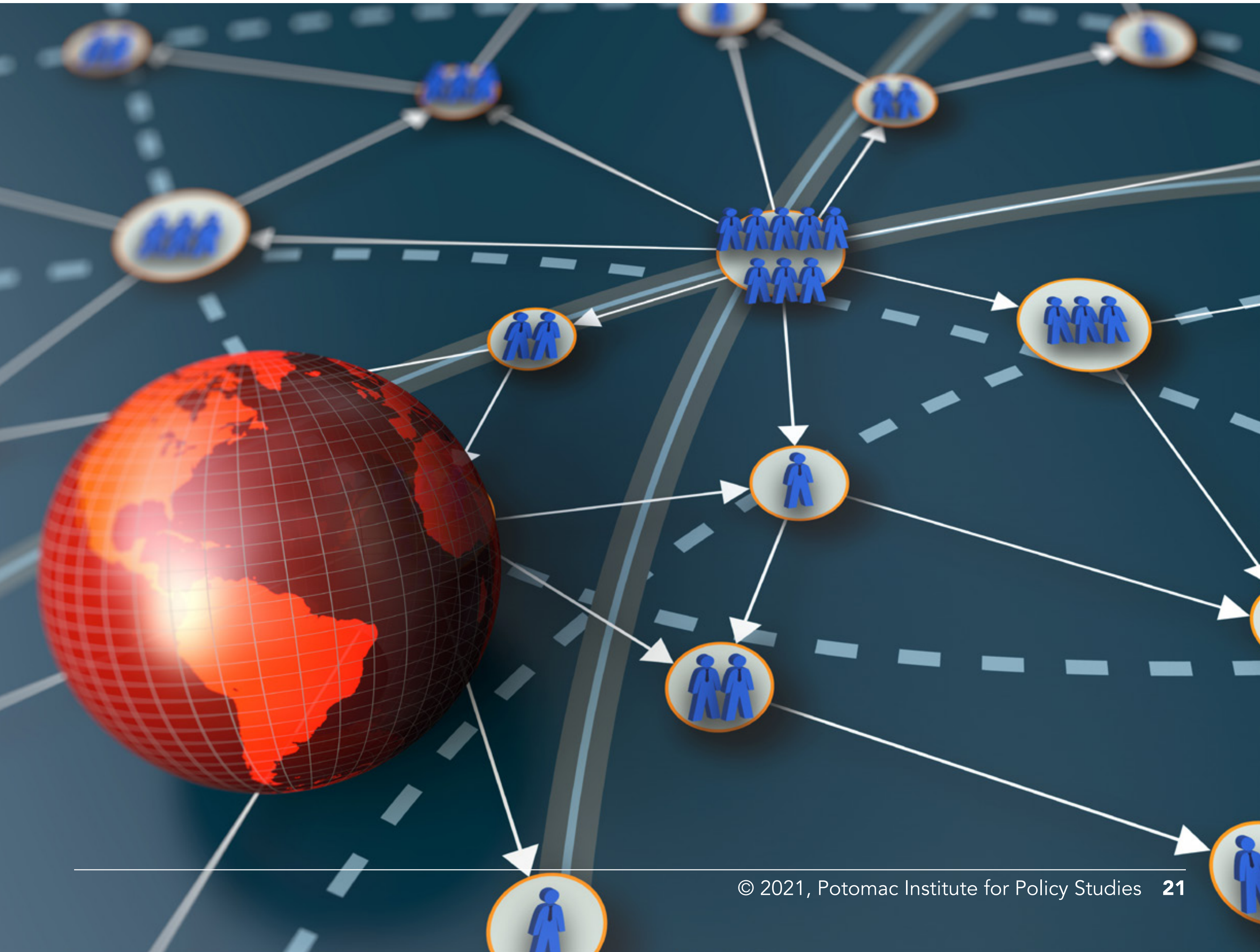
This strategy is fairly secure but requires a good deal of investment and effort. The United States already invests significantly more money and effort in its military compared to any other entity, but as Vietnam and Afghanistan have demonstrated, a superior military force by no means ensures easy or straightforward influence over other entities. Wars are risky, controversial, complex, incredibly costly, expend political capital and international prestige, and can devolve into a stalemate. Especially when dealing with a country from which we need critical resources, products, or services, the United States would have to be careful that when waging war or threatening destruction, that we do not threaten the very supply chain or critical infrastructure on which we rely. Moreover, this strategy would mean that in times of crisis when there is desperate competition for limited recourses, we would have to make foreign entities decide between giving up critical resources that they need or face destruction.

What is Critical in Full Control?

Each strategy has its benefits and downfalls, but ultimately, the United States will be in the most secure national security position if we have fully US controlled critical infrastructure. Creating this supply chain will not only increase national security, but will also enable increased investment into the US labor force and economy.

The question to consider now is, what should the United States consider critical infrastructure? The following five areas are suggested as components of critical infrastructure.

Critical Resources and Materials: Commodities necessary for building critical capabilities, including oil, iron ore, rare earth elements, etc.



Manufacturing Base that Can Scale Up and Adapt Production: A manufacturing base that consists of domestic factories that can respond to urgent needs. This component of critical infrastructure entails the understanding of the technology required to build vital products at scale, and to adapt manufacturing to assemble vital products—for example, the ability of a car manufacturing plant to build ventilators. This capability requires the knowledge and skill to build complex things at scale. The process of adapting and scaling production includes setting up the supply chain for raw materials; designing an assembly process with the appropriate tooling and fixtures, building, or securing test equipment; establishing testing and quality procedures; and working through materials handling and staffing.

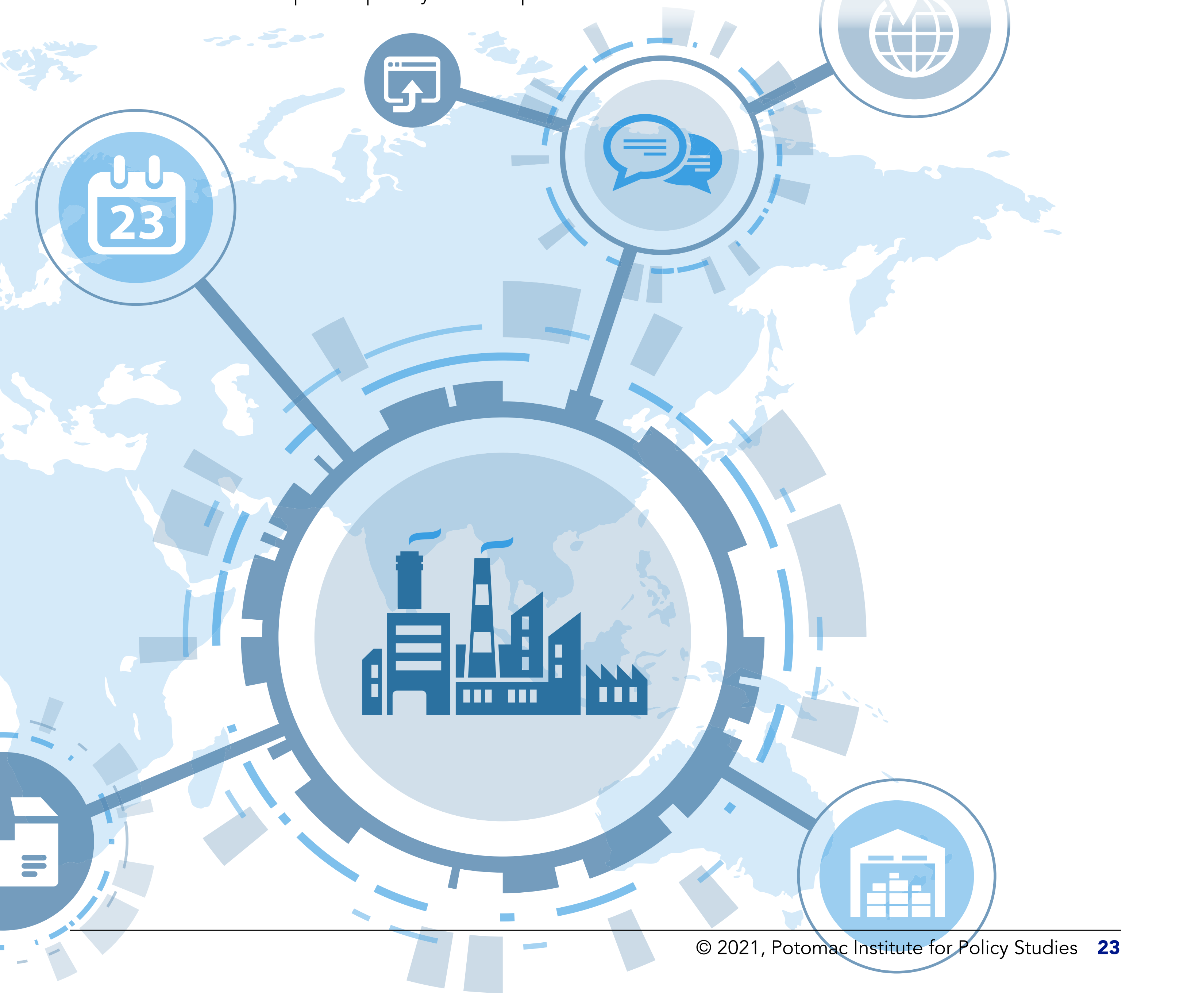
Skilled, Trained, Prepared Workforce: It is critical to have a skilled, trained, and prepared workforce that is ready to address a critical infrastructure challenge. This requires vast amounts of education, training, experience, and a culture that values those possessing critical skills. Creating such a workforce is likely to involve significant time and planning investments.

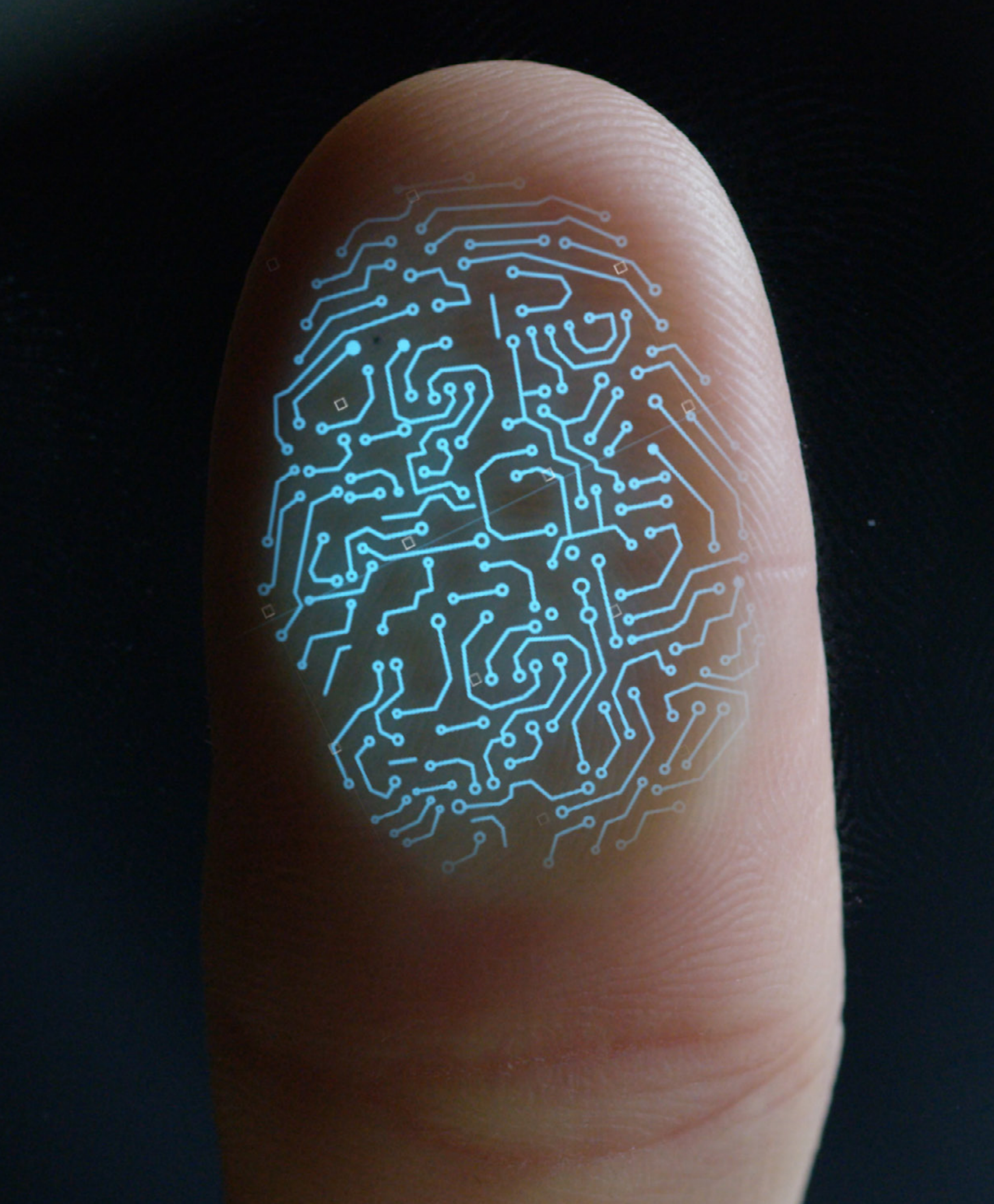
Specialized Manufacturing Capabilities: There are certain highly specialized manufacturing capabilities that are extraordinarily challenging to create from scratch. In times of need, the United States relies heavily on these specialized capabilities, such as microelectronics, bio-medical supplies and services, and space-related technologies, which must be sufficiently developed domestically.

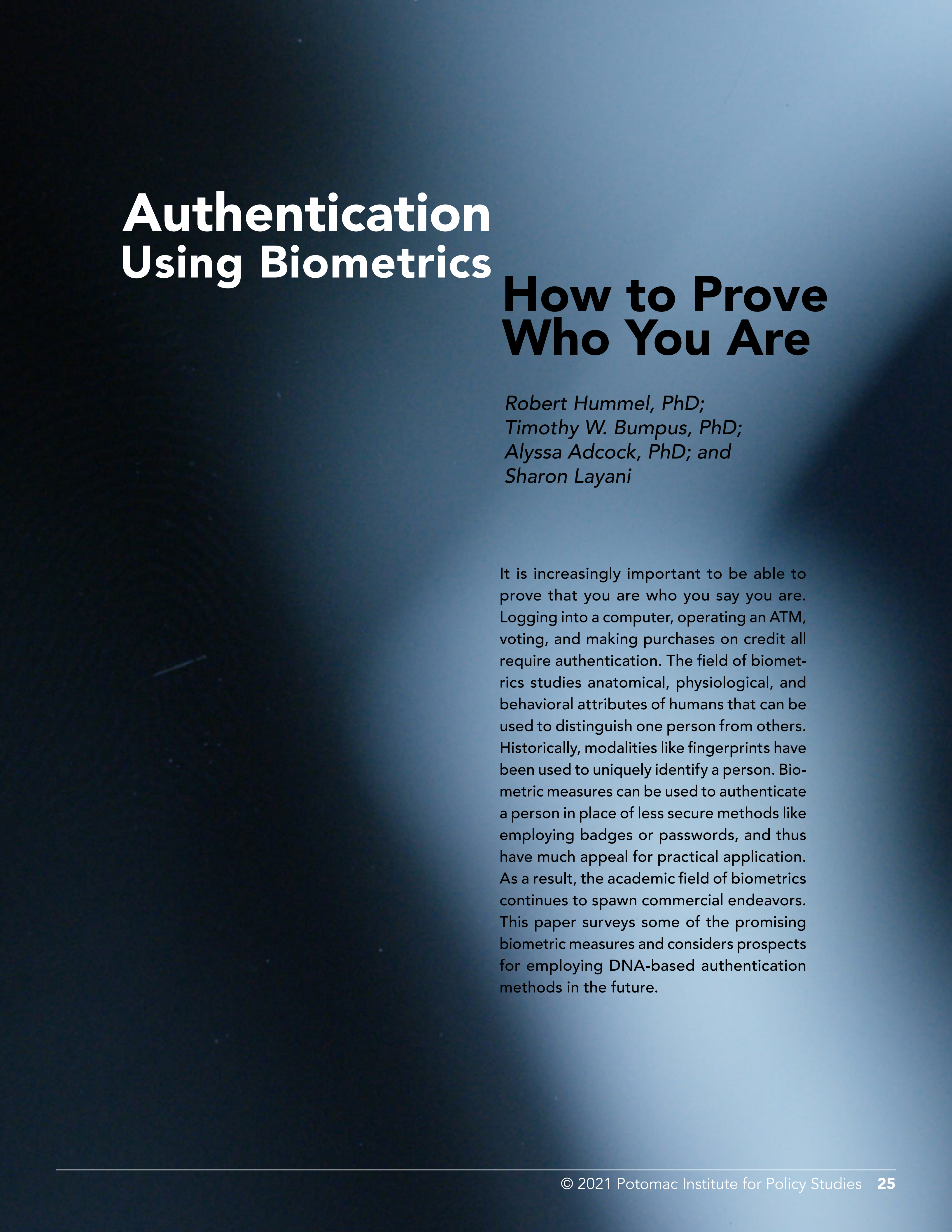
Strategic Inventory Reserves: Critical infrastructure includes reserves of critical products or materials that the United States cannot readily access or securely manufacture indefinitely. Given their focus on overall equipment effectiveness metrics, manufacturing plant managers are reluctant to install excess capacity. This means that factories are sized to handle the expected demand, with minimal surge capacity. The result is that when we experience a supply shock or sudden disruption in raw materials, components, or product supply, there is little buffer inventory available to absorb that shock. The United States had a buffer inventory of masks in a strategic stockpile, which was depleted during the H1N1 outbreak and never properly replenished. The United States should not even need to stockpile masks, as we should instead develop the capability to scale up their production. However, for products and materials where it is difficult to have secure control over the entire supply chain, strategic inventories that get promptly replenished should be considered a necessary component of critical infrastructure.

Conclusion

Of the strategies considered here, full US control of critical infrastructure supply chains is the recommended option. It will be necessary, however, to carefully discern which elements are truly critical. Achieving this strategy will require significant investment and effort, as the components of the critical infrastructure are currently inadequate. Restructuring to address the critical components, as described above, will take bold ideas and bold initiatives.







Authentication Using Biometrics

How to Prove Who You Are

Robert Hummel, PhD;
Timothy W. Bumpus, PhD;
Alyssa Adcock, PhD; and
Sharon Layani

It is increasingly important to be able to prove that you are who you say you are. Logging into a computer, operating an ATM, voting, and making purchases on credit all require authentication. The field of biometrics studies anatomical, physiological, and behavioral attributes of humans that can be used to distinguish one person from others. Historically, modalities like fingerprints have been used to uniquely identify a person. Biometric measures can be used to authenticate a person in place of less secure methods like employing badges or passwords, and thus have much appeal for practical application. As a result, the academic field of biometrics continues to spawn commercial endeavors. This paper surveys some of the promising biometric measures and considers prospects for employing DNA-based authentication methods in the future.

Introduction

It is hard to prove that you are who you say you are.

You have a name, and so you can tell people your name. But someone else could impersonate you by using the same name. What do you do if you have to prove that you are the person that you say you are?

Of course, we must prove it all the time. We sign documents, we provide passwords to log in, and we present photo IDs. Sometimes we are required to provide our social security number and date of birth, as though only we would know that information. Notaries check our government-issued picture IDs, as do the TSA officials at the airport. Increasingly, voting locales require some form of identification. Physical possession of a smartphone also acts as a personal identifier. Now, we can make purchases based on possession of our personal cell phone.

None of these methods of authentication are fool proof. For example, signatures morph over time and are forgeable. Databases of identification numbers are stolen. Passwords are hacked. Cell phones are stolen and unlocked. A determined impersonator can defeat any of these authentication approaches.

Identity fraud and identity theft are increasingly serious problems costing tens of billions of dollars per year in the US alone. All interactions with government, with financial institutions, and most interactions with businesses involve authentication as proof of identity. It is fundamental to our workings as a civilized society. The election security debate is mostly about trust in authentication. Technology, however, can provide solutions.

An unacceptable solution is to install a chip into every human upon birth. In lieu of this distasteful solution, society is increasingly turning to technology and employing biometrics to authenticate a person. Biometrics are unique physiological and behavioral attributes that can be used to identify individuals. These characteristics are individualized, relatively fixed, and recordable. Typically, they are also hard to forge. In what follows, we discuss the emerging possibilities for automated biometric authentication.

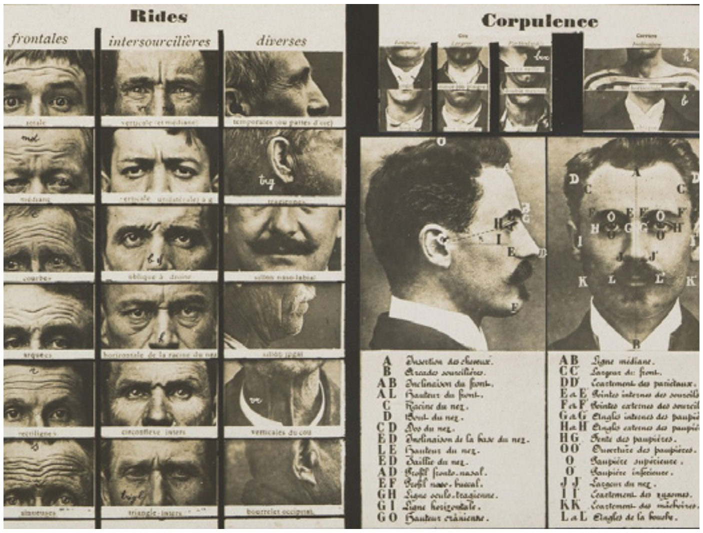
Ultimately, the most unique and immutable property of each individual is their DNA sequence. (Of course, identical twins have the same DNA sequence, but there are other markers to distinguish them.) By identifying an appropriate number of specific markers that vary across the population, but uniquely identify a particular individual, it should be possible to biochemically authenticate a person. With advances in biotechnology, we foresee a time when signatures can be replaced with fast and efficient biochemical tests.

Authentication of an individual is only one aspect of a broader set of applications of identity management. Biometrics can be used to identify a single person in a crowd or to label each person presented to a system. Authentication refers to a specific case, where a person is either an impersonator or not. Impersonation will be uncommon, but for many applications it is important that impersonators are deterred or caught.

The Biometric Database

The concept of using biometric data for authentication is to demonstrate that a set of traits unique to a person match a prior recorded registration of those traits. The pre-stored database associates identity with the biometric data. The recorded data can be stored locally to the individual in an unalterable form or can be accessed remotely. Information technology allows us to access such a database quickly, and the fact that the individual claims an identity means that accessing the appropriate record is easy and does not require a search (although a search is also generally easy).

The stored database needs to be secure, or else an imposter can change the associations. Moreover, stored biometric data will often be classified as personally identifiable information, protected health information, or individually identifiable health information. These categories of information are covered by regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and various state regulations, and so must be kept protected. While compromised passwords can be changed, compromised biometric information is not easily changed. Public key encryption and homomorphic access technologies to compare sampled data with the encrypted stored data are possible solutions to maintain security. However, compromises from hacking are always possible, and privacy concerns exist across much of civil society with respect to biometric technologies.



Alphonse Bertillon's Synoptic Table of Physiognomic Traits (ca. 1909).

Types of Biometrics for Authentication

Detailed ways of identifying people based on unique traits dates to the Bertillon System of 1879. Bertillon's system collected measurements to accompany a photograph of the subject and recorded the data on a filing card to track individuals in the criminal justice system. Bertillon's system captured five main measurements—the head length, head breadth, the length of the middle finger, the length of the left foot, and the length of the cubit (the length of the forearm).[1] While these measurements were not exactly unique and did lead to a few mistaken identity events,[2] they represent an early approach to systematic identity management. Today's "mugshot" is a direct hold-over from this approach.

More modern types of biometrics range across multiple modalities and can be categorized as external physiology, behavioral, and internal physiological. Table 1 lists examples of biomarkers that can be used as biometrics, within categories. Most can be used to help authenticate a person, to provide entry, or to permit authorized actions. Some biometrics provide binary data: they either match or they don't. Other biometrics are analog, and match only if the value is close enough. When used for authentication and referencing encrypted stored values, the associated encryption method needs to preserve "nearness" for such analog measures. For search, filtering, and identification applications, machine learning approaches might be useful in training the recognition system. For authentication, however, machine learning will be useful for finding features in the data that might be best extracted to do the comparison for verification, and a separate decision procedure is needed to decide if the features match the pre-stored features for each authentication instance.

In the next section, we provide more details for current and future biometrics that can be used for authentication, and in many cases other forms of identification.

Current and Future Directions

Certain biometrics for identity authentication have been around for ages and are mature technologies, while others are emerging and still under development. There is often little data about performance levels because the accuracy depends so heavily on the particular application, operating environment, and the distribution of the population being presented. The following is a survey of selected biometric modalities.

Face Recognition Systems

Humans use face recognition as the primary method of identifying people that they meet. Automated face recognition using image processing traces its roots to 1964 and the work of Bledsoe et al., who proposed identification based on 21 measurements.[3] Since then, face recognition has been a mainstay of computer vision research. Recognition often compares facial features based on the spacing of the eyes, the bridge of the nose, the contour of the lips, ears, and chin. Other approaches use features such as the residuals after a principal components decomposition of a cropped image of the face.[4] More recent developments include the use of machine learning for automated feature extraction and recognition against a database of stored faces.[5,6]

Commercial and government applications of face recognition are now standard. Some retail stores use facial recognition to identify returning shoppers.[7] Governments use facial recognition for border control. Non-cooperative access control for computers or physical portals can make use of face recognition. Authentication for logins to web accounts, such as Microsoft, Amazon, Google, and Facebook are valuable enhancements and explains why these companies have interest in face recognition. Other companies and agencies can monitor access to facilities using face recognition to supplement badge readers. Reports of widespread use of

Table 1. Examples of biomarkers that can be used as biometrics, within categories.

Category	Biometric	Description
External physiological	Voice	Identification based upon personal voice tracts
	Facial recognition	Identification by matching features from a map of facial features
	Fingerprints	Pattern recognition of the unique features of a fingerprint
	Palm prints	Similar to fingerprints, but not as widely used
	Hand geometry	Identification through the shape and dimensions of the hand
	Iris	Measuring the iris texture through visible and near-IR light to create a unique profile
	Ear shape	Similar to facial recognition but uses a detailed profile of the ear
	Scars	Considered a "soft" biometric identified along with marks and tattoos to identify an individual
	Eye veins	Using pattern-recognition on video images of the veins of the eyes
	Periocular	"Eye" recognition that includes the eyelids, eyelashes, eyebrows, tear duct, eye shape, and skin texture
	Odor	Characterizing and recognizing an individual based on their odor
	Footprint	Measuring the geometry, shape, and texture of footprints for identification
	Skin reflection	Using spectral reflectance of the skin for identification
Internal physiological	Sweat	Analyzing a profile based on amino acids and other compounds of each user from a sweat sample
	Blood and urine	Analysis of blood and/or urine samples. Blood samples can also be used to get DNA samples
	Microbiome	Using microbe data from stool, saliva, skin, and other collection sites, it has been shown that identification is possible and some samples remained stable for >80% of study participants after 1 year
	EEG/ECG	Taking EEG, ECG, or similar signals collected during a perception or mental task for identification purposes
	Tissue	Can include 2D ultrasound biometric systems. Direct tissue samples can also be used to get DNA samples
	Saliva	Saliva samples can be used to extract DNA samples
Behavioral	Typing habits	Based on monitoring how a user types, identity and mood can be identified
	Signature	Includes writing rhythm, acceleration, and habits
	Gestures	Generally captured from the face or hand; can classify and identify human motion
	Gait	Monitoring and modeling the way someone walks to identify them
	Touch screen tendencies	Integrating authentication into interaction based on personal tendencies on how a user touches a screen to ensure security
	Accelerometer data	A behavioral biometric identifier built around a user's movements
	How a device is held	Similar to touch screen tendencies and the accelerometer data, how a device is held can also build up a behavioral data set

facial recognition in China suggest population control. As a result of these and many other applications, there are many companies vying as suppliers of facial recognition technology.[8] Further, these technologies are available worldwide. Some face-searching tools are accessible to anyone as companies are able to capitalize on images others upload to the internet.[9]

Face recognition technology is controversial. Some contentious issues include government use of face recognition to track individuals, perform suspect law enforcement activities, repress disfavored ethnic groups, and generally violate privacy rights. Moreover, the technology has been shown to exhibit higher false positive rates for people of darker skin color,[10] and potentially other ethnic biases. As a result, legal restrictions have been placed on the use of face recognition in certain jurisdictions.

Due to years of research progress, face recognition works quite well when evaluated in laboratory settings. Typical benchmark reports show better than 99% accuracy,[11] others with error rate of less than 1%,[12] depending on the number of faces in the pallet of possibilities. Algorithmicists compete internationally: The GaussianFace algorithm developed in 2014 at The Chinese University of Hong Kong achieved facial identification scores of better than 98%.[13] In 2020, one facial recognition algorithm test had an error rate of 0.08%.[14]

For face recognition of images and video "in the wild," performance figures are less readily available. Performance must be measured in the context of the application and can vary with collection geometry and lighting. As an example, Apple claims that there is a 1-in-1,000,000 chance that a random person can unlock an iPhone using FaceID®,[15] but false rejection is less important because one can simply use a passcode in lieu of the biometric. Further, false rejections might not be evenly distributed across the population. Certain faces might be harder to authenticate, because they are too nondescript.

Fingerprinting

Fingerprint recognition is one of the oldest and most developed biometric recognition methods. Latent fingerprint identification has been used forensically since at least the 19th century.[16] Today, automated fingerprint recognition for authentication is regularly used for access control. The FBI maintains the Fingerprint Identification Records System and uses the Integrated Automated Fingerprint Identification System (IAFIS) to match fingerprints against the database. Fingerprint-based access control systems for computer access or physical portal control are available commercially.[17] Many laptops now have built-in fingerprint readers to control login access and use of a password manager, although the software generally allows for a password-based backup in case the fingerprint identification falsely rejects the user. As another example, the airport screening company Clear uses biometrics to authenticate people, with fingerprints as one of the biometrics that can be used.

Historically, fingerprints were collected using ink impressions on cardboard cards. Now, fingerprints can be collected using optical approaches, and can even be obtained by contactless methods. Contact systems can use an image, or measure conduction from a capacitive surface. Certain smartphones now use ultrasonic sensors to collect fingerprints. Contactless fingerprint technologies include commercially available contactless fingerprint scanning technologies, with at least four mobile (smartphone-based) apps and two stand-alone contactless devices on the market.[18] Contactless devices generally require that the fingers are in close proximity to the reader, but a fingerprint of a German defense minister was famously digitally recreated from photos.[19]

The technology for recognizing fingerprints can use a direct comparison of the stored image of the fingerprint against the scanned print, invariant to a certain amount of variation of position and angle. However, this approach can fail to align the features accurately, and so the established method of recognizing fingerprints is by observing specific features (such as loops, whirls, and arches), categorized manually, or extracted automatically using image processing. Biometric identification research continues to include developing improvements to fingerprint recognition, especially for contactless technologies.[20]

The accuracy of fingerprint identification is highly variable, and controversial.[21] For authentication, most systems will establish a loose threshold, with the assumption that imposters will be rare. Crime-solving using fingerprints is well established, but often makes use of other evidence to help narrow the search and improve the apparent accuracy of the fingerprint identification.

Automated Signature Verification

The earliest surviving signature is from 3100 B.C.E.,[22] signifying the importance of signatures for authentication. Automated signature recognition can either be static, i.e., comparing one total signature image to another, or dynamic and can involve additional data such as the coordinates, pressure, azimuth, and inclination. Automated signature recognition has been a continuing research application of image processing, both historically,[23] and more recently.[24] Signature verification is heavily used in banking, real-estate, and government applications. Numerous software vendors supply software systems to support signature identification.[25,26]

There are currently many studies looking at the accuracy of signature recognition. However, scores need to be interpreted in the context of whether one is attempting to reject random forgeries or skilled forgeries.[27] For true positives, there is the issue that signatures naturally change over time and thus require certain tolerances to be accepted. There are famous examples of forgeries that have evaded detection by experts (at least initially) such as the Hitler Diaries.[28] Often celebrities' signatures sold online have been found to be faked. Research goals would hope to make automated signature verification as good as expert manual verification, but current systems are likely not that good.

Hand Geometry and Palm Prints

In addition to fingerprint recognition, hand geometry (the use of hand measurements) as a biometric has received much research interest.[29,30] Hand geometry can be combined with palm prints for higher accuracy, using such measures as the area of the hand, and the length/width of fingers, and palm print features such as lines, wrinkles, minutiae, and delta points.[31] Using IR sensors, one can combine information from the structure of veins in the hands and fingers.[32,33] The goal is to develop a contactless verification system wherein one could wave a hand that would then be evidence of one's identity.[34,35]

While much of the hand and palm recognition development is in academic research, since 2013 the FBI has maintained the National Palm Print System of millions of palm prints. Many anticipate rapid growth in the market sector for hand and palm print biometrics, with companies proliferating in hardware, software, and services.[36]

These systems claim high accuracy, with one system giving greater than 96% accuracy even against blurred palm images.[37] Still, accuracies have to be interpreted according to the application and the probability of imposters. But since palm prints are easier than fingerprints, if they are indeed sufficiently stable, it would seem to be a very favorable identify verification modality.

Iris Scans and Retinal Scans

The human eye is highly variable across individuals, and certain features are stable over time, thus providing a useful biometric marker. Passports already record eye color, but this provides relatively little specificity across the population.

The pattern of capillaries and blood vessels on the back of the retina (of either eye) can be used as a far more specific biometric. First patented in 1935,[38] the concept was made practical by a device in the mid-1970s,[39] and has since been commercialized and used by government agencies. Since the eyeball must be placed against an eyepiece, and the scan involves low-intensity illumination by an infrared source, the technique is invasive, and only practical for cooperative identification. While spoofing is difficult for this biometric, the retinal pattern can change over time or due to disease or stroke. For this and other reasons, retinal scans for identification have not seen widespread use.

Instead, the iris has proved a more useful biometric. The iris, the annular region surrounding the pupil of the eye which defines the color of the eye, is composed of connective tissue and muscle fibers, and provides a pattern that is specific to the individual. It can even distinguish between identical twins. Proposed in 1936[40] and first patented in the 1980s,[41] an algorithm to perform pattern recognition of irises was licensed to a variety of companies throughout the 1990s.[42] A profusion of different collection methods and matching algorithms have led to increasing practical use, particularly as replacement for physical passports at airport control portals, but proposed for e-commerce and other uses as well.[43] Both theoretically and in laboratory tests, irises are sufficiently variable as to allow unique identification among billions of people.[44]

Iris scans pose challenges to becoming the universal biometric, despite their appealing specificity. While it is possible to obtain an iris scan from several meters away, the optics and collection geometry have to be exquisite, and thus the process is expensive. This is true even for cooperative collection. Mirrored or dark sunglasses and custom textured contact lenses can thwart collection, and eyelashes and reading glasses can get in the way of passive, non-cooperative collection systems.

Still, with improvements in optical systems and digital cameras, as well as faster and more affordable processing capabilities, iris scan technology can be expected to become far more prevalent in the future. Once registered, it provides an excellent way to prove one's identity.

Other Modalities

The field of biometrics is large and growing. Here are some of the biometric fields that weren't discussed above:

- Voiceprints: A spectral decomposition of spoken or recorded speech, plotted as a function of time.
- Typing dynamics: Based on keystroke patterns on a telegraph, computer keyboard, or touchscreen on a smart phone
- Gate and body motion: Style of walking as gleaned from video or smart phones accelerometers, distinctive body motions; patterns of how a device is held
- Body odors: Volatile organic compounds (VOCs) that, for example, dogs can use to identify people
- Chemical effluents: Data from sweat, blood, urine, or analysis of a person's microbiome
- Electrical activity: Electroencephalograms/ Electrocardiographs[45] ("heart prints")
- External physiology: Ear shape, scars, tattoos, periocular and footprint data, and skin reflection

Many modalities can be used in combination to increase specificity. Impersonators can be thwarted if they don't know which combination of modalities will be used for authentication.

Biometrics Using DNA

The ultimate biometric is one's DNA. Our identity is wrapped up in the 23 chromosomes contained within the nucleus of every cell across our body.[46] These molecules are the core of our identity, and the three billion base pairs contained therein define us as unique individuals based on the many small variations within that code.

Thus, one way to authenticate a person is to sequence their genome and compare the sequence to a pre-stored sequence. While sequencing the entire genome is expensive and time consuming, new solutions that might reduce the cost significantly, and reduce the time required to a mere hour or less.[47]

However, it is not necessary to sequence the entire genome to identify a person. It suffices to find a few dozen locations that vary from individual to individual and sequence those sections alone. This can be done by targeting specific sites, amplifying a few dozen base pairs at each of those locations, and reading off the resulting sequence to obtain identifying information. Currently, forensic DNA analysis uses sites of the human genome with short tandem repeats (STRs), which are specific sites where there are a variable number of repetitions of short sequences of bases where the number of repetitions varies from person to person. A similar approach might also be possible using single nucleotide polymorphisms (SNPs). Using twenty[48] or so such sites (across the chromosome pairs), one can obtain a quite unique identifier of a person, and the process can be accomplished much faster and more economically than sequencing the entire genome.

Sequencing-free genotyping is also being developed. The approach utilizes CRISPR-Cas technologies to precisely target specific sites and then uses biochemical signal generation methods to indicate detection of specific genomic patterns without actually sequencing the region.[49] While still very much in the research stage, these strategies may enable the generation of functionally unique identifiers, while further reducing the time and cost required.[50]

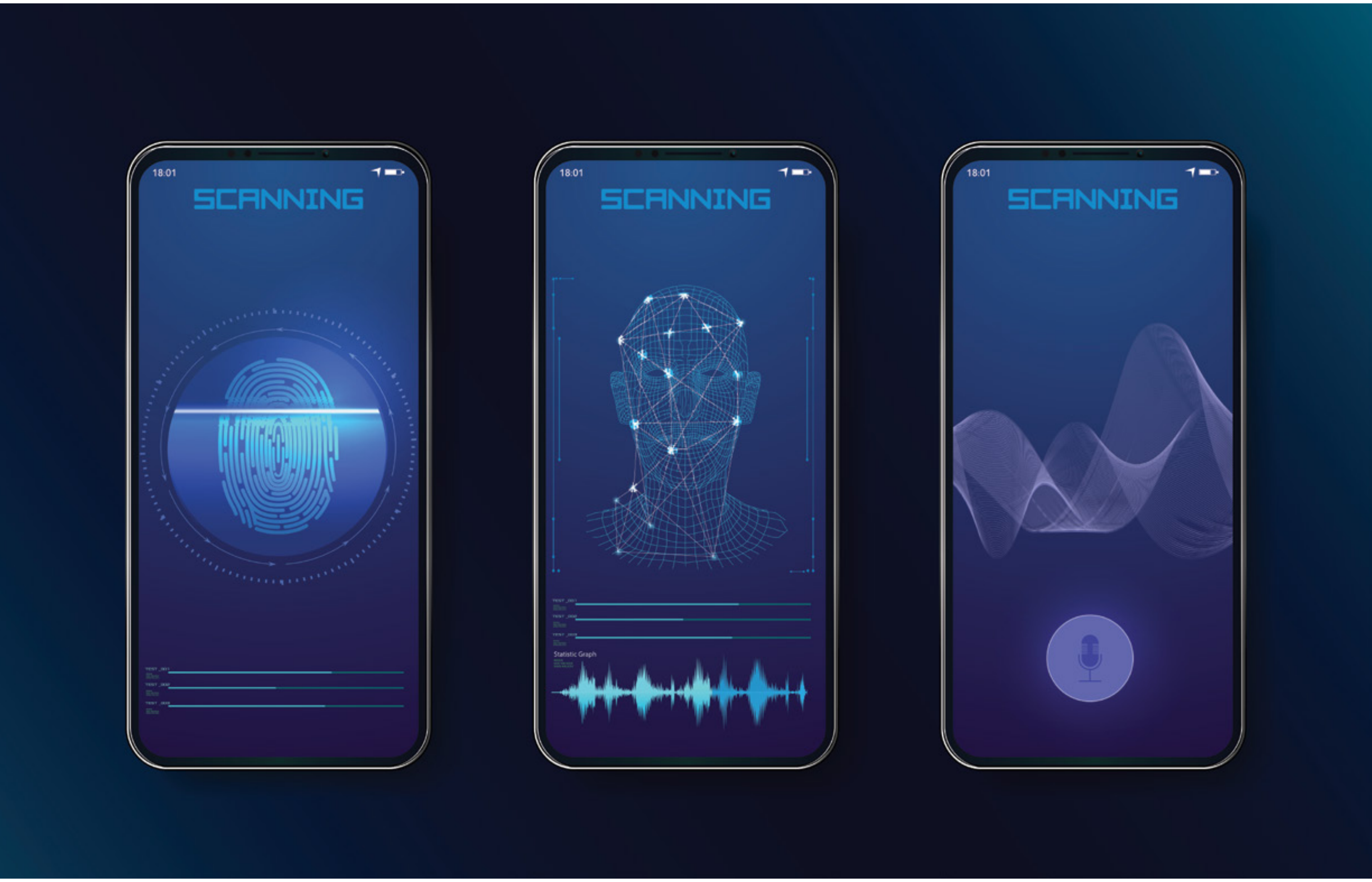
Though there are automated ways of performing sequence and genotype analyses, there are currently no mass-produced affordable analyzers. Further, the chemistry is such that the sequencing of the variable sites will still take a few minutes at least. Thus, DNA biometrics for access control will take too long for most purposes. But for signature verification in place of a notary, say for large purchases or the issuance of passports or other government-IDs, the fact that the verification might take a few minutes (or even an hour) is not a large impediment. After all, signatures are rarely validated in real time. Instead, the challenge is the engineering and production of sufficient numbers of analyzers to make such systems commonplace, and the supply of necessary chemicals.

Indeed, since DNA is the gold standard in identity verification, it is likely that it would be used as the certifying biometric to register other identifiers, which are then used for day-to-day access and verification.

Conclusion

Given that passwords and multi-factor authentication approaches to authentication are painful and not particularly secure, biometrics offer a better solution. There are many different modalities to choose from, with the possibility of using multiple biometrics to improve specificity. For each modality, there are technical, cultural, and implementation issues. Fingerprint and face recognition technologies have improved but are far from perfect. Retinal and iris scans seem to work quite well, but have not been widely deployed. Other more exotic modalities are not particularly selective. Yet the need to authenticate oneself for security, whether for access or authorization, continues to increase.

Increasingly, there will be a desire to develop non-invasive, non-cooperative biometric capabilities. In this way, authentication can happen without requiring tokens, passwords, credit cards, or other interventions that take time and effort. People can then gain access to a facility or a computer without interruption. They can be authorized to take specific actions based on their identity. Checkout at stores can happen without a chipped credit card. Autonomous ride share vehicles can authenticate their passenger automatically. Health records can be accessed securely. The convenience and security of passive authentication will be compelling for a large variety of audiences and applications.



Since most biometrics are a reflection of one's DNA, and one's DNA is the only truly immutable feature that identifies a person, the ultimate way to authenticate someone is to verify that their DNA matches the registered version of their DNA. Today, this can be done by genotyping or genomic sequencing, which are both relatively lengthy and costly processes. However, in the future, using new technologies, it might be possible to do the verification affordably in minutes. Developing this capability will take research and investment. It will likely take standards to determine the portions of the genome that can be used to distinguish between individuals. It behooves federal agencies to accelerate the development of such capabilities, for both national security and economic dominance applications. The best way to collect a sample for DNA analysis, whether cooperatively or non-cooperatively, remains undetermined. The capability might not come to fruition or might only be used for extraordinary identifications, but the science and technology for DNA-based identification is clear, as are the advantages.

Endnotes

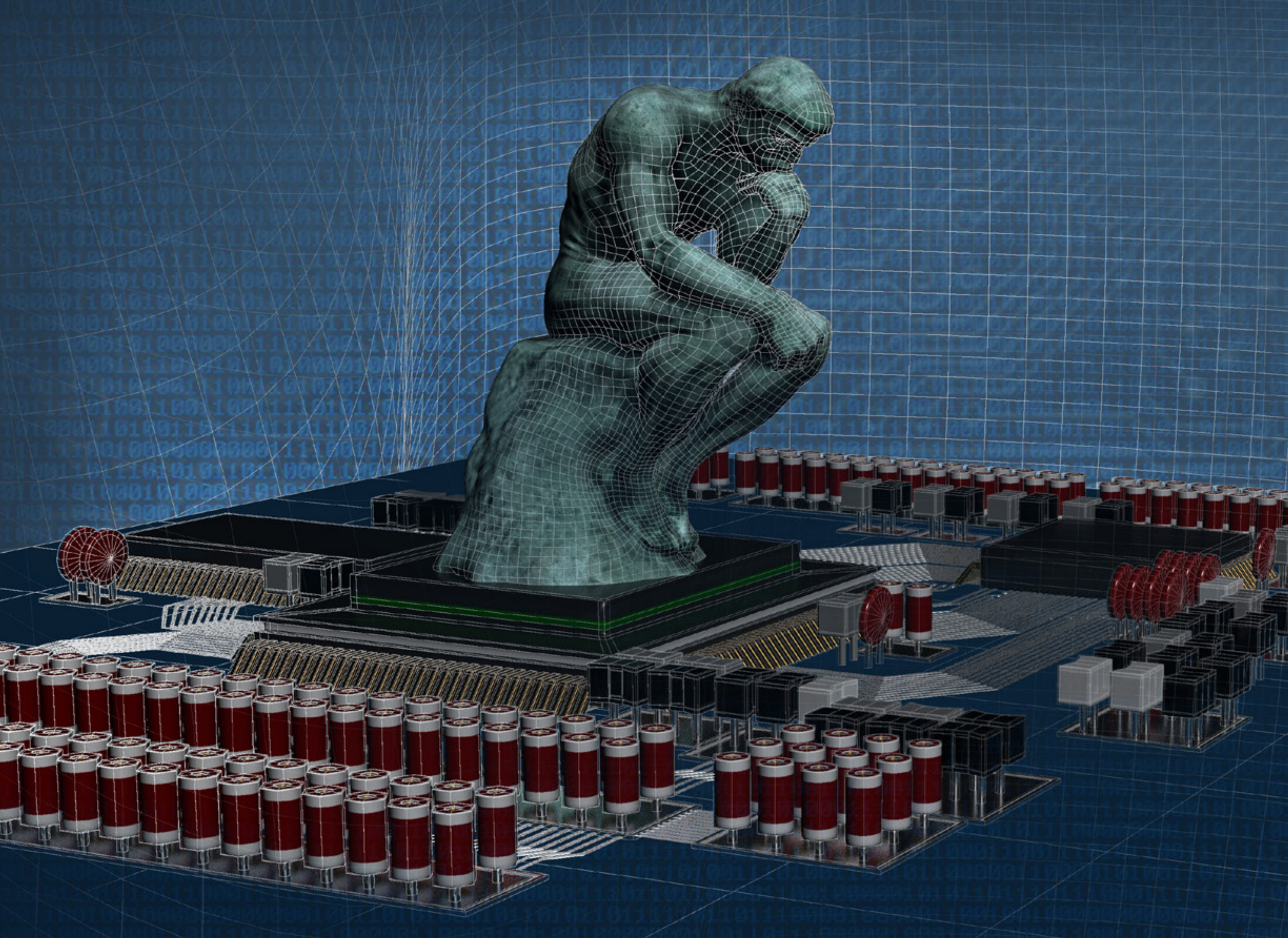
1. "The Bertillon System," U.S. National Library of Medicine, April 20, 2021, https://www.nlm.nih.gov/exhibition/visibleproofs/galleries/technologies/bertillon.html.
2. "Fingerprints: The Convoluted Patterns of Racism." Dickinson College. April 20, 2021, http://dh.dickinson.edu/digitalmuseum/exhibit-artifact/babes-in-the-woods/fingerprints.
3. Woodrow Wilson Bledsoe, "The Model Method in Facial Recognition," Panoramic Research Inc., Palo Alto, CA, Rep. PR1 15 (47) 1964.
4. MatthewTurk and Alex Pentland, "Eigenfaces for Recognition," *Journal of Cognitive Neuroscience* 3(1) 1991: 71-86, https://www.face-rec.org/algorithms/PCA/jcn.pdf.
5. Rajeev Ranjan, et al., "A Fast and Accurate System for Face Detection, Identification, and Verification," *IEEE Transactions on Biometrics, Behavior, and Identity Science* 1(2) 2019: 82-96. https://ieeexplore.ieee.org/document/8680708.

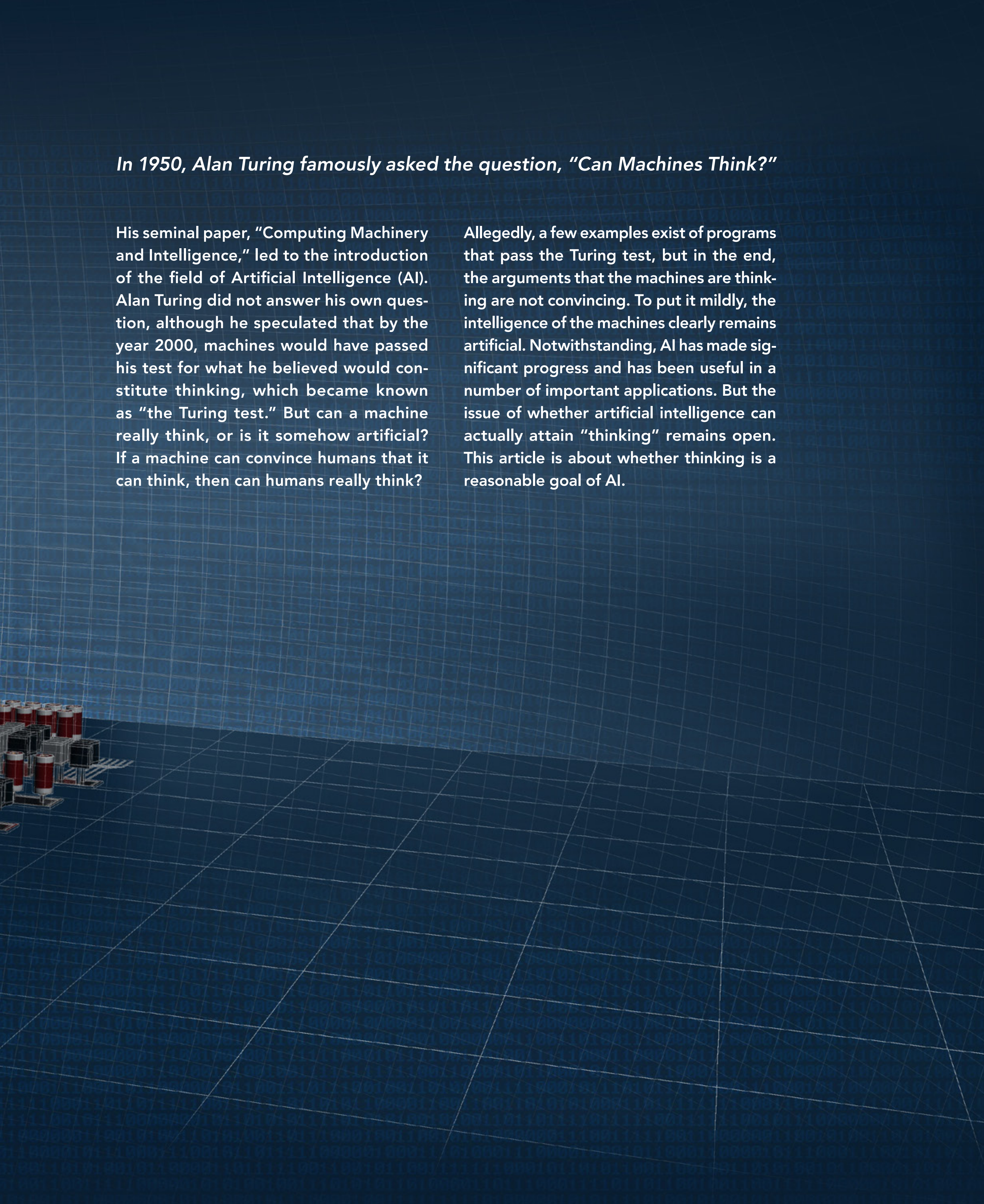
6. Rajeev Ranjan, et al., "Hyperface: A Deep Multi-task Learning Framework for Face Detection, Landmark Localization, Pose Estimation, and Gender Recognition." *IEEE Transactions on Pattern Analysis and Machine Intelligence* 41(1) 2017: 121-135. https://ieeexplore.ieee.org/document/8170321.
7. Sergio Mannino, "Council Post: How Facial Recognition Will Change Retail," *Forbes* May 8, 2020. https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/?sh=19df789f3daa.
8. Aashish Mehra, "Facial Recognition Market Worth $8.5 Billion by 2025." *Markets and Markets* December 2020. https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp.
9. Drew Harwell, "This Facial Recognition Website Can Turn Anyone Into a Cop – Or a Stalker," *The Washington Post*, May 14, 2021, https://www.washingtonpost.com/technology/2021/05/14/pimeyes-facial-recognition-search-secrecy/.
10. Sarah Henderson, "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software." National Institutes of Standards and Technology, May 18, 2020. https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.
11. InsafAdjabi, et al., "Past, Present, and Future of Face Recognition: A Review." *Electronics* 9(8) 2020: 1188. https://doi.org/10.3390/electronics9081188.
12. "Facial Recognition: Top 7 Trends (Tech, Vendors, Markets, Use Cases & Latest News)," *Thales Group* April 10, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/facial-recognition.
13. "Facial Recognition: Top 7 Trends".
14. William Crumpler, "How Accurate Are Facial Recognition Systems – and Why Does It Matter?" Center for Strategic & International Studies, April 14, 2020. https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter.
15. "About Face ID Advanced Technology." Apple Inc., February 26, 2020. https://support.apple.com/en-us/HT208108.
16. "Automated Fingerprint Identification System (AFIS) Overview - A Short History," Thales Group, April 5, 2021. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history.
17. For instance, IDEMIA's MorphoWave system collects data from four fingers at once. https://www.idemia.com/contactless-fingerprint.
18. "NIST Study Measures Performance Accuracy of Contactless Fingerprinting Tech." National Institute of Standards and Technology, May 19, 2020. https://www.nist.gov/news-events/news/2020/05/nist-study-measures-performance-accuracy-contactless-fingerprinting-tech.
19. Alex Hern, "Hacker Fakes German Minister's Fingerprints using Photos of Her Hands." *The Guardian* December 30, 2014, https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands.
20. For example, the Center for Identification Technology Research" (CITeR), an NSF Industry-University Cooperative Research Center (IUCRC), and affiliated universities research biometric recognition and credibility assessments. Some of this work features looking at the algorithms for touchless fingerprints. https://iucrc.nsf.gov/centers/achievements/ai-helps-shift-touch-id-to-touchless.
21. William Thompson, et al., "Latent Fingerprint Examination," *AAAS* September 15, 2017. https://www.aaas.org/sites/default/files/reports/Latent%20Fingerprint%20Report%20FINAL%209_14.pdf?i9xGS_EyMHnIPLG6INIUyZb66L5cLdlb; "Report on the Erroneous Fingerprint Individualization in the Madrid Train Bombing Case." *FBI Forensic Science Communications* 7(1) 2005. https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/jan2005/special_report/2005_special_report.htm;Ulery, Bradford T., et al. "Accuracy and reliability of forensic latent fingerprint decisions," *Proceedings of the National Academy of Sciences* 108(19), May 10, 2011. https://www.pnas.org/content/108/19/7733.
22. "'First Signature' Tablet Hits the £140,000 Mark at Bloomsbury Auctions," *Antiques Trade Gazette* July 13, 2020. https://www.antiquestradegazette.com/print-edition/2020/july/2451/news/first-signature-tablet-hits-the-140-000-mark-at-bloomsbury-auctions/.
23. Roger NortonNagel and Rosenfeld, Azriel, "Computer Detection of Freehand Forgeries." *IEEE Transactions on Computers* C-26(09) 1977: 895-905, https://doi.org/10.1109/TC.1977.1674937.
24. Leading researchers in this area include Donato Impedovo & Giuseppe Pirlo, the Central Police University's Department of Forensic Science in Taiwan, CEDAR (Center of Excellence for Document Analysis and Recognition, University at Buffalo, SUNY), and Stanford University's Law and Policy Lab Automated.
25. The leaders in the marketplace include Microsoft Azure, Parascript, ProgressSoft, Biometric Signature ID, Certify Global Inc., and ISign Solutions Inc. See also: "The Signature Verification Market Is Expected to Register a CAGR of 24.77% during the Forecast Period 2019." *Cision PR Newswire* September 11, 2019. https://www.prnewswire.com/news-releases/the-signature-verification-market-is-expected-to-register-a-cagr-of-24-77-during-the-forecast-period-2019--300916140.html.
26. "Signature Verification Market: Growth, Trends, and Forecast (2020 - 2025)." Mordor Intelligence May 12, 2021. https://www.mordorintelligence.com/industry-reports/signature-verification-market.
27. Javier Galbally, et al., "Accuracy Evaluation Of Handwritten Signature Verification: Rethinking The Random-Skilled Forgeries Dichotomy." 2017 IEEE International Joint Conference on Biometrics (IJCB), 2017: 302-310, doi: 10.1109/BTAS.2017.8272711.

28. "Forger Who Duped the Media with Hitler's Diaries," *The Irish Times* February 24, 2013, https://www.irishtimes.com/news/forger-who-duped-the-media-with-hitler-s-diaries-1.1124037.
29. Stephen Mayhew, "Explainer: Hand Geometry Recognition." *Biometric Update* May 13, 2021, https://www.biometricupdate.com/201206/explainer-hand-geometry-recognition.
30. Arun Ross, et al., "A Prototype Hand Geometry-Based Verification System." *Proceedings of 2nd Conference on Audio and Video Based Biometric Person Authentication* 1999: 166–171, http://web.cse.msu.edu/~rossarun/pubs/RossHand_AVBPA99.pdf.
31. Ajay Kumar et al., "Personal Verification Using Palmprint and Hand Geometry Biometric." In: Kittler J., Nixon M.S. (eds) *Audio- and Video-Based Biometric Person Authentication*. AVBPA. Lecture Notes in Computer Science, vol 2688. (Heidelberg: Springer, Berlin) 2003, https://doi.org/10.1007/3-540-44887-X_78.
32. Yingbo Zhao and Ajay Kumar, "Human Identification Using Palm-Vein Images." *IEEE Transactions on Information Forensics and Security* 6(4) 2011: 1259-1274, doi: 10.1109/TIFS.2011.2158423.
33. Kashif Shaheed, et al., "A Systematic Review of Finger Vein Recognition Techniques." *Information* 9(9) 2018: 213, https://doi.org/10.3390/info9090213.
34. J. Svoboda, et al., "Contactless Biometric Hand Geometry Recognition Using a Low-Cost 3d Camera." International Conference on Biometrics, 2015, https://www.semanticscholar.org/paper/Contactless-biometric-hand-geometry-recognition-a-Svoboda-Bronstein/044264a61868bc4e0efb8b501f326cb93f9fade0.
35. Vivek Kanhangad, et al., "A Unified Framework for Contactless Hand Verification." *IEEE Transactions on Information Forensics and Security* 6(3) 2011: 1014-1027, https://doi.org/10.1109/TIFS.2011.2121062.
36. "Palm Recognition Biometrics Market Overview." *Research Nester* February 25, 2021. https://www.researchnester.com/reports/palm-recognition-biometrics-market/2865.
37. Shihab Shawkat et al., "The New Hand Geometry System and Automatic Identification." *Periodicals of Engineering and Natural Sciences* 7(3) 2019: 996-1008, http://pen.ius.edu.ba/index.php/pen/article/viewFile/632/368.
38. Robert B. Hill, "Apparatus and Method for Identifying Individuals through their Retinal Vasculature Patterns." United States Patent, Application Number 759,901, Filed January 17, 1977. https://patents.google.com/patent/US4109237A/en.
39. Robert Hill, "Buzz," "Retina Identification," in *Biometrics: Personal Identification in Networked Society*, ed. Anil K. Jain,et al., (US: Springer) 1996: 123–41, https://doi.org/10.1007/0-306-47044-6_6.
40. "Modalities." The FBI Biometric Center of Excellence, May 13, 2021. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-center-of-excellence-1/modalities-1.
41. Stephen Mayhew, "Explainer: Speaker Recognition," *Biometric Update*. Accessed May 12, 2021, https://www.biometricupdate.com/201206/explainer-iris-recognition.
42. Stephen Mayhew, "Explainer: Speaker Recognition."
43. Luiz Nogueira, "Singapore to Replace Passports with Facial and Iris Detection." *Olhar Digital* October 28, 2020, https://olhardigital.com.br/en/2020/10/28/noticias/singapura-substituira-passaportes-por-deteccao-facial-e-de-iris/?gfetch=2020%2F10%2F28%2Fnews%2Fsingapore-to-replace-passports-with-facial-and-iris-detection%2F; Aaron Brandley, "Next Step in Mobile Security: Iris Recognition," *Epic eCommerce* October 7, 2016, http://epicecommercetools.com/2016/10/07/next-step-in-mobile-security-iris-recognition/.
44. John Daugman, "Probing the Uniqueness and Randomness of IrisCodes: Results From 200 Billion Iris Pair Comparisons," *Proceedings of the IEEE* 94(11) 2006, https://www.cl.cam.ac.uk/~jgd1000/ProcIEEEnov2006Daugman.pdf.
45. João Ribeiro Pinto, et al., "Towards a Continuous Biometric System Based On Ecg Signals Acquired On The Steering Wheel," *Sensors* 17(10) 2017: 2228, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676989/.
46. With the notable exception of red blood cells, which are enucleated in mature form.
47. Bradley J. Fikes, "New Machines Can Sequence Human Genome in One Hour, Illumina Announces," *San Diego Union Tribune* January 9, 2017, https://www.sandiegouniontribune.com/business/biotech/sd-me-illumina-novaseq-20170109-story.html#:~:text=Focus%3A%20New%20machines%20can%20sequence,in%20one%20hour%2C%20Illumina%20announces&text=SAN%20FRANCISCO%20%E2%80%94%20DNA%20sequencing%20giant,a%20couple%20of%20years%20ago. May 13, 2021, and https://www.illumina.com.
48. Twenty STR loci are currently maintained in the United States' CODIS database. "CODIS and NDIS Fact Sheet." FBI, June 8, 2016, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet.
49. Sequencing-free testing technologies are being pursued by Mammoth Biosciences (https://mammoth.bio) and Sherlock Biosciences (https://sherlock.bio).
50. Many companies are pursuing biotechnologies related to sequencing and biochemical tests; for a list of several relevant companies, see: Mark Terry, "Top 10 Gene Sequencing Companies by Revenue," *Biospace* Nov 29, 2019, https://www.biospace.com/article/top-10-gene-sequencing-companies-by-revenue/.

Can Humans Think?

Robert Hummel, PhD





In 1950, Alan Turing famously asked the question, "Can Machines Think?"

His seminal paper, "Computing Machinery and Intelligence," led to the introduction of the field of Artificial Intelligence (AI). Alan Turing did not answer his own question, although he speculated that by the year 2000, machines would have passed his test for what he believed would constitute thinking, which became known as "the Turing test." But can a machine really think, or is it somehow artificial? If a machine can convince humans that it can think, then can humans really think?

Allegedly, a few examples exist of programs that pass the Turing test, but in the end, the arguments that the machines are thinking are not convincing. To put it mildly, the intelligence of the machines clearly remains artificial. Notwithstanding, AI has made significant progress and has been useful in a number of important applications. But the issue of whether artificial intelligence can actually attain "thinking" remains open. This article is about whether thinking is a reasonable goal of AI.

Turing well understood that he needed to define the terms "machine" and "think." For a machine, he knew precisely what he meant, which is what we now know as a "Turing Machine." In the same paper, he notes that the model of a machine that he has in mind is universal. Today, every modern digital computer is, for all practical purposes, an instantiation of a Turing machine.[1]

The definition of "to think" is much murkier. In Turing's interpretation, he substitutes a test, the Turing test, which is a version of the "Imitation Game," but amounts to asking the machine to convince a panel of humans that the machine is actually human. It should do this by responding to queries and conducting a written conversation. The "Watson" program developed by IBM to play the game "Jeopardy" is amazingly good at information retrieval and might be considered quite good at convincing people that it is human. After all, it won in certain games of Jeopardy. But even Watson makes mistakes that provide evidence it is not human.

The problem is that the substitution of "to think" with the Turing test is not the same as confronting the question of what it means to think. Admittedly, it is too hard to define "thinking," as it takes one down the path of trying to understand consciousness and intuition and intelligence and what it means to be human. For good reasons, Turing avoided the question. Clearly, humans can think. And yet, we don't know what it means to think.

We may have trouble defining "to think," but we can agree on certain things that are not thinking. For example, looking up information by brute force from a table of information is not thinking.

As an illustrative example, elementary school students memorize the multiplication table. They learn, for example, that nine times nine (9 X 9) is 81. They know this (or memorize this) due to an entry in a matrix that is the multiplication table. This is not thinking. However, if they forget, or refuse to memorize the table, then they might compute that 9 X 9 = 9 X (10 – 1) = 90 – 9 = 81. That reasoning involves some amount of thinking.

But let us agree that table lookup is not thinking. It can be performed automatically without thinking. It follows that a Turing Machine cannot think. This is because, by definition, a Turing Machine is a finite state machine that implements lookups based on a finite lookup table. Because a Turing Machine simply implements lookups, it can't think. And since every existing digital computer is subordinate to the Turing Machine model, no digital computer can think.

Now, let us suppose that a digital computer manages to truly satisfy the Turing Test. That is, imagine that a digital computer can perform discourse and reasoning such that it can convince most humans that it has the same intellect and reasoning ability as any human. Let's assume that it has access to experiences and memories equivalent to a typical human's memory. The mere fact that such a computer can thoroughly simulate a human and "think" in a way that convinces humans that it is equivalent to a typical human, implies that human thought is equivalent to or subordinate to a digital computer. That is, the implication is that the human brain is no more powerful than a Turing Machine.

But we agreed that a Turing Machine can't think, because it simply implements a finite lookup table. It might be a complicated lookup table, but it still isn't thinking. So, if indeed a digital computer can simulate a human, it follows that a human can't think.

Could it be that all humans are merely convincing other humans that they can think, but not really thinking? Can humans think?

The suggestion then, is that all human thinking and indeed intelligence, can be cast in terms of tables and precise steps dictated by a program of a computer.[2] There have been ideas of other types of computation that might be involved, such as distributed parallel processing, but AI posits that table lookups giving rise to von Neumann processing (as it has come to be known) should suffice to mimic human intellect.

The question casts doubt on aspects of the field of Artificial Intelligence (AI). While AI only purports to mimic intelligence (and thus produce "artificial" intelligence), practitioners would like to think that their AI programs show evidence of thinking. When Turing asked whether machines could think, the field of AI had not yet been invented. But when McCarthy coined the term "artificial intelligence" a few years later, and researchers met in the first AI conference, the hope was that the application of logic by computer programs could prove theorems and thus mimic the thinking aspects of intelligent human beings. The implication, however, is that humans don't really think—that all thinking is actually based on table lookups.

To date, AI has achieved many successes in terms of assisting humans in performing tasks. But there is arguably a lack of "thinking" that can be ascribed to any AI program. Marcus and Davis, leading AI researchers, bemoan the lack of convincing thinking of AI programs in their book "Rebooting AI." This is not to decry the usefulness of AI to a range of problems and applications. However, it questions whether AI based on digital computers can be interpreted, in any sense, to provide thinking abilities. That is, AI might not be producing any true intelligence, at least as implemented to date. Instead, AI attempts to mimic thinking, in the same way that humans are purportedly deluding themselves into thinking that they can think.

At issue is whether a digital computer as an implementation of a Turing Machine can emulate the human brain. If so, the human brain could then be thought of as its own form of a Turing Machine, albeit one with a great deal of complexity. Do humans perform all thinking by state transitions from one of a finite number of states to another state, based on stimuli (i.e., inputs) from a finite alphabet of possible inputs?

There are two possible answers to this question:

One possibility is that yes, humans are a finite state machine, similar to a Turing Machine, but that the complexity is so large that it seems like they are really thinking, when in fact it is simply that the alphabet and the number of states is so large that it can't really be understood as simple lookups.

The other possibility is that the human brain is more complicated than a Turing Machine, and is performing steps that are not part of the Turing Machine model.

Alan Turing was well aware of this dilemma. He considered—and rejected—a number of possibilities that thinking required something more complex than a Turing Machine. Thus he adopted the first alternative, that thinking is simply a very complex version of a finite state computer.

And indeed, modern digital computers are Turing Machines (modulo having finite memory stores) but can have incredibly complex state spaces and huge alphabets of possible inputs. For example, modern machines can perform floating

WHAT IS A TURING MACHINE?

A Turing Machine is a deliberately simple model of computation that is nonetheless powerful enough so as to model what are seemingly far more complex machines. A Turing machine is a finite state machine that can read and write to a linear store (a "tape") of symbols from a finite alphabet, and that performs table lookups based on the current symbol that is read on the tape together with the current state, thereby writing a new symbol onto the tape, moving the tape either left or right, and adjusting the current state to potentially a new state, among the finite set of possible states. The essential point is that the Turing machine performs lookups using a table of state-transitions, dependent on symbols read from the tape.

point multiplications in nanoseconds. It would not seem that these operations are based on lookups. But in fact they are. Underlying arithmetic operations are algorithms, performed in binary arithmetic, that invoke additions and shifts.[3]

Does complexity hide the fact that everything in life is actually based on finite lookup tables, and thus there is no real thinking?

The other possibility is that a Turing Machine is not powerful enough to encompass thinking—that a different model of computation is required to actually achieve what we would truly consider thought. By implication, the human brain is more complex than an extremely complex Turing Machine. For example, deep neural networks, which seem so related to neurons and dendritic structures that accumulate inputs, when implemented in digital computers and graphical processing units that use floating point arithmetic to implement matrix multiplications and activation functions, are in fact just Turing Machine lookups that are inadequate to explain what is happening in the brain.

If the goal of AI is to actually emulate a thinking human being, then it is going to need something other than a computer equivalent to a Turing Machine. There are many possibilities. One possibility is to attempt to emulate the brain. However, it is erroneous to assume that the electrical properties of neurons and their graphical structure of connectivity (the connectome) is sufficient to explain the workings of the brain. And even if it were true, the pattern of firings of neurons is far different from the binary signals used in digital computers. It is very possible that the best way to emulate the brain is to get a brain.

We can list many other possibilities for computers that differ from a Turing Machine model, that might have some chance of thinking. Some of these ideas were considered by Turing and rejected. Others, like a quantum computer, were not

Table 1. Different approaches to extending the Turing Machine model to attempt to model a machine that can "think."

Technical Approach	Comments
Add randomness	As Turing points out, one can simulate in a Turing Machine, simply by computing successive digits of pi (π) and using them as a pseudo random number generator.
Parallelism	Most versions of parallelism can be accomplished with a Turing Machine, by simply executing each processor in turn. For simultaneous writes, one can simulate the winning value using randomness.
Non-determinism	Can be accomplished on a Turing Machine, but just in a different complexity class.
Analog processing	Difference between representing real numbers versus all rationals is slight, and not likely to be important. Analog is hard to do in silicon.
Spike train processing	Whereas analog computing normally thinks of neurons as simply encoding the rate of firing, actual neurons have patterns of firing such that time of arrival of each pulse at a synapse is functional. This could be accomplished using specialized hardware. But it is really just more complex analog processing, where spike trains can be represented by vectors of reals.
Quantum computing	Not likely a brain function. Aim of quantum computers is not thinking, but complexity class reduction for certain algorithms (e.g., Shor's Algorithm).
Multiple generative adversarial networks competing on different aspects of intelligent behavior	Has shown remarkable abilities to produce fake images and create realizations of complex statistical random fields, but is implemented using a Turing Machine model. Does the system understand anything about what it creates?
Implement machine simulated emotion	One reviewer calls this Artificial Stupidity. Would emotions lead to better intelligence? Or just different intelligence. Moreover, not only do we not understand intelligence, we don't understand much about emotions.

conceptually available at the time. Table 1 lists some possibilities and comments on each. But just because a model of computation is different from the Turing Machine model does not mean that it is capable of thinking. The only existence proof, as best as we can tell, is the human brain. And even then, depending on how one defines "to think," we can't be absolutely sure that humans can think.

Turing's conclusion, after rejecting a number of possibilities, was that sufficient complexity (which he foresaw) would enable computers to convincingly mimic humans (pass his subjective test). Computers are now at least as intricate as his vision of complex machines and have arguably (at times) convinced panelists that there was a human in the background, but machines have not achieved what we would rationally consider "thinking."

Everyone believes that artificial intelligence is among the top research areas that will be impactful and/or provide transformative technology of the future. China has announced a desire to lead the world in AI research by 2030. None of the discussion above is intended to deny the importance of AI research. However, **the goal of that research should be applications that augment or automate tasks normally conducted by humans**. Humans are often slower and less effective at tasks that can be automated by a computer.

If the goal is to build a machine that can truly think, then a different kind of machine will be needed. Sadly, current implementations of "neural networks" and machine learning follow the Turing Machine model, and thus, are simply complex deterministic machines that follow the rules of a finite state machine and a finite transition table. If one believes that neural networks and machine learning are steps toward mimicking the human brain, they should understand that they are at best miniscule steps in that direction, and fail to move beyond implementation ability using the Turing Machine model.

This discussion, and the understanding of the workings of any computer that implements the Turing Machine model, suggest that it is a fool's errand to try to show that an existing computer can think, at least in the way that humans can think.

For Further Reading

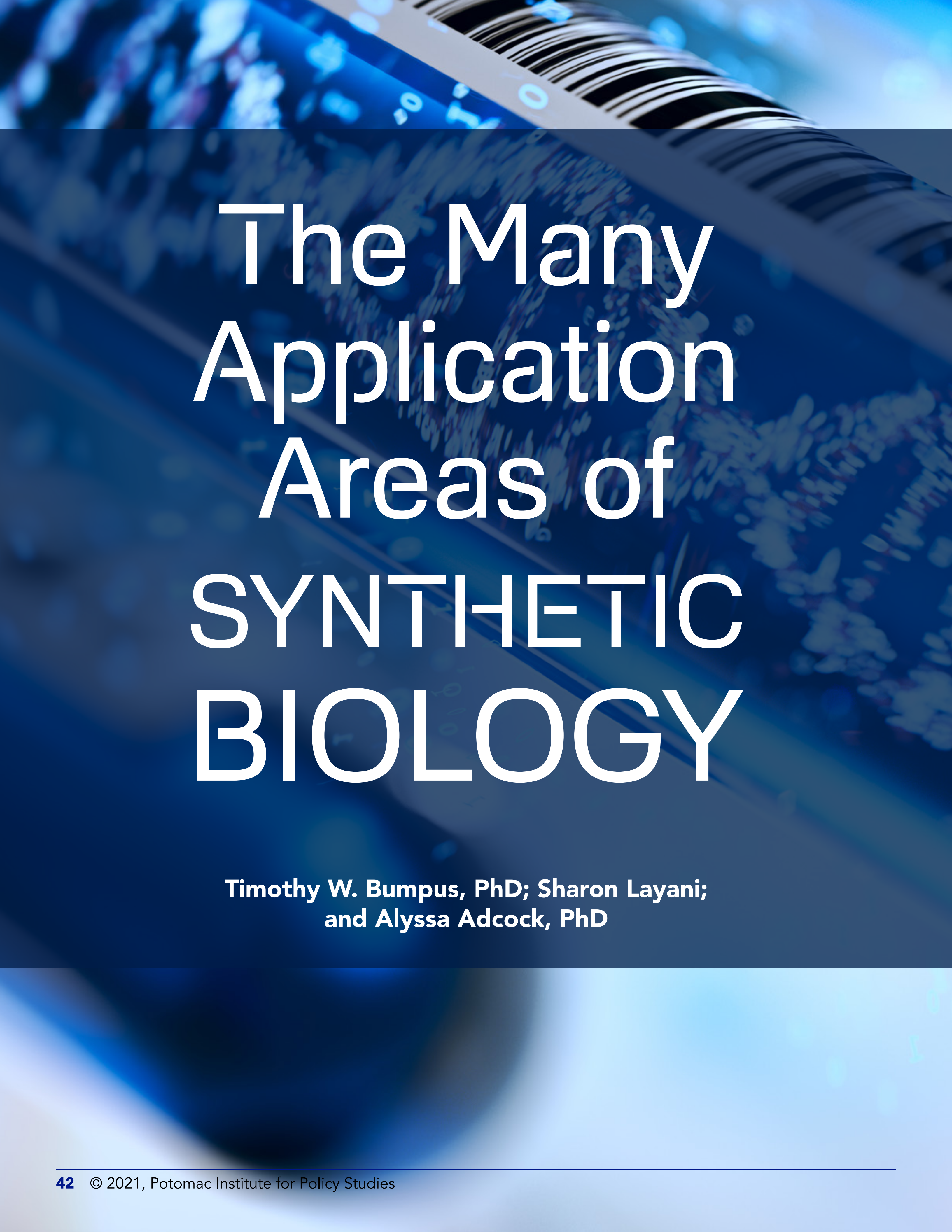
Alan Turing, "Can Machines Think?" *Mind* LIX(236) 1950: 433-460, https://doi.org/10.1093/mind/LIX.236.433.

Paul Austin Murphy, "Alan Turing Believed the Question 'Can Machines Think?' to be Meaningless," *Becoming Human: Artificial Intelligence Magazine*, https://becominghuman.ai/alan-turing-believed-the-question-can-machines-think-to-be-meaningless-7a4a8887b220.

G. Marcus and E. Davis, Rebooting AI: Building Artificial Intelligence We Can Trust (New York: Random House) 2019, https://www.amazon.com/Rebooting-AI-Building-Artificial-Intelligence-ebook/dp/B07MYLGQLB.

Endnotes

1. In fact, although a Turing Machine is seemingly incredibly simple, it is slightly more powerful than existing digital computers, because it assumes it has an infinite store of memory, whereas real computers have a finite amount of memory. In practice, however, the amount of memory is such that existing digital computers are essentially equivalent to a Turing Machine.
2. Von Neumann himself was interested in other models of computation for intelligent behavior.
3. When performing addition of two binary numbers, each "digit" involves two addends and a carry bit, or three bits total, for eight possibilities. The result is a single bit, the summand, and a carry bit, or two output bits. This can be accomplished using a lookup table with eight entries, and two output bits. Thus, all arithmetic operations, including multiplications and divisions, are algorithms applying lookup tables.



The Many Application Areas of SYNTHETIC BIOLOGY

Timothy W. Bumpus, PhD; Sharon Layani;
and Alyssa Adcock, PhD

The burgeoning field of synthetic biology promises myriad applications that would mark a major shift in the lives of people worldwide. In the same way that microelectronics transformed society beginning in the latter half of the 20th century, synthetic biology and its applications are likely to again transform society's relationship with products and nature. Such profound change arises because through synthetic biology, humankind can reach beyond exploiting nature and its biological factories as developed through eons of evolution and begin designing biological products with structures and properties dictated entirely by us.

The advertised applications of these new technologies include developing new classes of therapies and vaccines (which we have begun to see with the mRNA COVID-19 vaccines), the ability to cure previously intractable diseases, or the possibility of eliminating genetic diseases. Much focus has been placed on the possibility of editing human embryos (so-called germline editing), which could result in inheritable changes to the human DNA pool, and the consequent dangers. However, there are other applications that do not require heritable modifications (somatic cell editing), and still others that do not modify the human genome at all. Our interest here is in the applications outside of human germline editing. Further, there are important applications beyond medical interventions, to include environmental care, agriculture and food production, materials production and manufacturing, energy management, and (even) information technology. With so many diverse applications, it is useful to discuss some of the possibilities in each area.

Introduction

The term "synthetic biology" was coined over a century ago. Since then, synthetic biology has grown into a diverse, multidisciplinary field that leverages tools, techniques, and ideas from biology, chemistry, engineering, computer science, medicine, bioinformatics, and many other fields. Closely allied to bioengineering, synthetic biology aims to create new biological elements or redesign existing processes found in nature. Recent scientific breakthroughs and commercial tools have ushered in new advancements and opportunities. The development of these tools and the maturation of synthetic biology as an academic field has led to the discovery of applications and the formation of companies.

The current field of synthetic biology is the culmination of decades of scientific breakthroughs and technological advancement. From the discovery of DNA and its function, to uncovering its double-helix structure, unraveling the genetic code, constructing a reference human genome, economizing genetic sequencing, and the more recent developments in genome editing, these basic research discoveries have enabled innumerable applications. In his recent book, author Walter Isaacson describes the CRISPR-Cas-9[1] "genetic scissors" discovered by 2020 Nobelists Jennifer Doudna and Emmanuelle Charpentier as transforming "the future of the human race"[2] and flags the many thorny ethical issues this transformative technology brings to the fore. Most notable of these are the issues surrounding germline editing, which would alter the inheritable human genome.[3] However, these concerns, though extremely serious and justified, should not forestall the use of synthetic biology in its many other applications.

Depending on what one includes in the breadth of synthetic biology, market potentials for applications (in annual US dollar amounts) are estimated to be in the tens of billions for new applications over the next few years.[4] Venture capital funds [5] and foundations[6] have been established to support and accelerate developments. Dozens of early-stage start-up companies have been formed in the US, while at the same time basic research continues in academic and corporate research laboratories to provide greater understanding of the opportunities afforded by synthetic biology. Bringing applications to fruition and commercializing synthetic biology products, however, will require considerable work and technological expertise.

It is clear that the field is in its infancy, and thus the full range of applications remains largely unexplored. Many applications, as yet unimagined, might be possible as the field expands. For example, it is possible to modify DNA to admit replacements for one or more of the four nucleotides, or to expand the number and kind of nucleotides.[7] One such experiment used eight different nucleotides.[8] Such an expanded genetic alphabet will surely allow researchers to explore new possibilities and may result in new proteins and polynucleotides with previously unattainable, or even unimaginable, properties and functionalities. While some researchers work to build new biological systems and capabilities from the ground up, others are starting with the nearest facsimile nature already possesses and then through directed evolution teaching that protein new, alternative functions. This allows for biology's catalysts (enzymes) to do more of the work that was once done by teams of human chemists.

In this article, we discuss the current activities in and progress across a number of synthetic biology application areas. In all cases, however, much more development can be expected—leading to a range of new products, many not envisioned here. As the academic field continues to organize and expand, the range of applications for exploration will likewise expand, through startups and industries. Our focus here is on what is known now about applications and their logical extensions.

Human Health Care

In 2020, we learned how messenger RNA (mRNA) can be designed to instruct human cells to produce a protein based on a portion of the SARS-CoV-2 virus that causes COVID-19, thereby teaching the immune system to produce antibodies (the body's major element of immunological defense) prior to an infection. The rapid development of this novel vaccine has profoundly impacted society and promises future vaccines and therapies based on an analogous approach. Based on rapid genetic sequencing, computational biology, and biomanufacturing, the Moderna and BioNTech/Pfizer vaccines have become advertisements for the success of synthetic biology.

The production of mRNA vaccines is but one of the successes of synthetic biology in biomedicine. Engineered yeast have been used to produce semi-synthetic artemisinin for an anti-malarial drug,[9] and production of the diabetes drug Januvia® uses a new directed evolution derived enzyme to replace older, environmentally harmful manufacturing processes.[10] A new form of cancer treatment called CAR-T cell therapy[11] (for Chimeric Antigen Receptor T-cell therapy) uses synthetic biology to alter T-cells harvested from the patient's body to attack tumors. The success of CAR-T cells has sparked interest in applying the same technique to other immune cell types, such as natural killer cells.[12] Other interventions under development use engineered probiotics to augment the body's immune functions through the gut's reservoir of commensal bacteria.[13] Yet other developments use synthetic biology to generate 3D scaffolds upon which to culture cells and regenerate bones, tissues, or potentially even whole organs.[14]

Successes to date just scratch the surface of possibilities for synthetic biology in the design of novel diagnostics, therapeutics, vaccines, and preventative health care. Future applications include further vaccine development (potentially again using mRNA vaccines) to thwart a host of viral afflictions (for example, the common cold), prophylactic healthcare, treatments for metabolic disorders, and stopping emerging infectious diseases *before* they become pandemics. Further, it can be applied to uncover biologics that counter the effects of aging on the human body.[15]

Because market forces will drive demand, we can envision that synthetic biology will also serve the interests of performance enhancing drugs, supplements, and production of unapproved pharmaceuticals. In these cases, efficacy is likely to be a mixed bag as it will be based on understanding the biological mechanisms of the human body, which are immensely complex. Synthetic biology will be a component of the research that increases our understanding, but it is not guaranteed that all biologics will provide safe and effective results, regardless of the method of production.

Going forward, we can expect synthetic biology to be the crucial enabler for precision medicine.[16] Precision healthcare, which includes individualized medicine, is often regarded as the future of human healthcare. Precision health would revolutionize the practice of medicine by tailoring diagnostics and therapies to individuals based on their unique genetics, microbiome, diet, lifestyle, environment, or individual disease characteristics. Diagnostics and therapeutics may then be tailored based on those particulars, making use of synthetic biology where necessary and appropriate.

Earth's Biological Environment

The tools of synthetic biology can be applied by humans to augment, improve, and better exploit the earth's biological environment. That environment consists of the delicate ecosystems that surround us and with which humans must coexist. Over the millennia, humans have profoundly impacted the biological environment, often warring against pests and threats while exploiting other plants and animals for our benefit. Synthetic biology provides unique opportunities and capabilities to further these influences on the environment, ideally in beneficial ways.

Fighting undesirable, disease carrying, or invasive species may now be accomplished through synthetic biology, in preference to the introduction of competitor species.[17] For example, genetically modified mosquitoes are being developed to curtail the spread of mosquito-borne diseases, which remain a serious threat to human health.[18] Field trials have recently begun in the Florida Keys to test both the efficacy and effects of such approaches in natural ecosystems. A biopesticide approach to controlling locust infestations has also been proposed, using synthetic biology to reprogram the insects' microbiome and disrupt essential genes via bacteriaphages.[19] Gene drives (a genetic construct that alters the genetic makeup of a particular species by inserting a small piece of DNA into an individual that then spreads and dominates reproduction of genes in subsequent generations) and viral vector delivery systems are highly modular approaches that will likely find many new applications, to include addressing infestations, limiting the spread of zoonotic diseases, or culling invasive plants or animals.

Other applications of synthetic biology to altering the earth's biological environment can involve generating microbes with desirable properties.[20] Such developments might portend an ability to clean up oil spills or remediate other forms of environmental and xenobiotic pollution. Application of such microbes may hasten the degradation of plastics in landfills,[21] promote nitrogen fixation, improve soil productivity, and reduce fertilizer usage,[22] or even reduce atmospheric greenhouse gas levels.[23] Synthetic biology can also enable the development of biological markers that can be used as sensors, to detect the presence of contaminants or pollutants. One such research development involves

bacterial infused beads that can be spread across the surface of a field and which fluoresce green in the presence of trinitrotoluene (TNT) vapors to detect buried landmines.[24] Indigenous plants might also be modified in a similar way, so as to include sensors that can be observed optically or by other spectroscopic means.

In the realm of multicellular creatures, there have been serious thoughts about bringing back the wooly mammoth through synthetic biology,[25] based on genetic information found in preserved DNA strands. Such techniques could also be used to restore recently extinct species or re-establish species that are nearly extinct. This could include, for example, rescuing certain species of trees from a blight, or treating a species of beneficial bees to resist specific diseases.

Admittedly, many of these applications come with profound risk. Humans have often caused grave environment damage, frequently as a result of good intentions gone awry. Modern interventions using synthetic biology must be carefully tailored to the specific problem and have safeguards built in to prevent undesirable effects. These are challenging issues, spanning scientific disciplines and jurisdictional regimes. Special caution is warranted because many forms of synthetic biology involve unleashing life forms that replicate and proliferate.

Agriculture and Food Production

While controversial today, genetically modified organisms (GMOs) have been produced historically through animal husbandry and agricultural practices involving plant breeding. However, now, it is possible to apply synthetic biology approaches to add or subtract genes to plants and animals to produce desirable benefits. Viral transduction, which uses a virus to transfer genetic material, has been used to produce hardier plants.[26] Famously, Monsanto developed seeds (such as soybeans) that are immune to the deleterious effects of the weed killer Round Up® thereby allowing for greater crop yields.

Less notorious uses of synthetic biology for agricultural purposes are found in the development of fertilizers rich in engineered bacteria to improve crop yields,[27] and the development of artificial food additives using custom fermentation.[28] The latter products can include sugars, flavor simulants or enhancers, dietary supplements (such as flavonoids and terpenoids), and oils and fats (lipids) for food enhancement. Using knowledge of human taste and olfactory receptors, it might be possible to develop new flavors of foods more pleasing to human senses. Looming on the horizon, and of much interest in agriculture, is the use of synthetic biology to culture meat directly from engineered cells, obviating the need to butcher animals. Already, the FDA has approved a fish food that has been developed through the editing of a bacteria's genetic makeup that produces a flour-like aquaculture feed.[29] While seemingly far from growing a synthetic beef steak, numerous companies and research labs are in a race to develop cultured meat with properties identical to animal products.[30] Some predict that within five years, consumer cultured meat products will be commonplace.[31] Others believe that getting the texture, grain, and mix of fats to properly mimic actual butchered meat will prove more difficult. The technology to make it happen, however, includes a number of synthetic biology concepts, as well as 3D printing technology using multiple constituent cell types.

Similarly, other food products, to include fruits and vegetables, might be cultured from media using biological processes that do not rely on natural soil and sunlight. Efficiencies in food production using synthetic biology to culture cells, whether meat or vegetable, extend beyond the rate and aesthetics of production. Consider the situation of a contained bioenvironment, such as a long-duration manned space capsule, or an Antarctic outpost. Production of fresh food via cell/tissue culture, as opposed to long term storage or resupply using long transport lines, can offer major advantages. Further, by using recaptured water to reconstitute freeze-dried media, the total weight of the food supplies can be significantly reduced. Beef, for example, is around fifty percent water, so by culturing cells in reconstituted media to produce a juicy New York Strip, you could eliminate up to half the weight of the beef supply, while supplying a superior fresh food product.

Synthetic biology might also be able to detect and reduce issues of food spoilage. Biological sensing mechanisms embedded into the packaging may monitor the state of the food degradation, such as detecting milk spoilage.[32] Today, some foods are irradiated to prolong their lives, which is an indiscriminate way of adjusting the biological makeup. Additives or packaging designed and manufactured via synthetic biology would be able to more precisely counter processes that cause food spoilage, producing foods that require less in the way of refrigeration to achieve long shelf lives. Such biologic sensors and additives could dramatically transform food distribution and storage.

Materials Production and Manufacturing

Biological processes produce a large variety of proteins with diverse structural and chemical properties. From delicate silk thread fibers with immense tensile strength, to the cellulosic structures to enable trees to reach their towering heights, natural biology can construct and manufacture an amazing array of useful structures. Through synthetic biology, humans may also start to make use of biological processes to produce specially designed materials and construction methodologies. By replacing or modifying traditional processes such as chemical synthesis and commodity manufacturing, we are likely to design novel materials and new applications, all the while improving the efficiency and reducing the environmental impact of manufacturing.

Though biomanufacturing remains in development, both existing materials companies (for example Dupont) and innumerable start-ups are exploring how best to leverage biological processes to generate products. Bio-cements, for example, are being produced to create materials and adhesives for construction that reduce its carbon footprint.[33] There is also a long history of attempting to produce silk thread, normally associated with spiders and silkworms, which thanks to synthetic biology is beginning to achieve meaningful success.[34] Commercial-quality nylon 6 yarns, films, and engineered bioplastics are the intended products of a joint venture that produces bio-renewably derived caprolactam (a precursor to these products).[35] These replacement products are intended to be more sustainable and environmentally friendly. The Department of Defense has awarded a Manufacturing Innovation Institute, called BioMade, to the Engineering Biology Research Consortium led by Cargill to "identify and innovate on shared challenges in scaleup and downstream processing to further strengthen the US economy in the production of bioindustrial products."[36]

Researchers are using synthetic biology to develop cell-free protein synthesis methods. Proteins are typically produced in cells, where cellular membranes render these biochemical wunderkinds largely inaccessible. Synthetic biology now permits protein synthesis without cell membranes, to scale up production of therapeutic small molecules[37] and glycoproteins,[38] fine chemicals, biofuels, and even bio-enabled smart materials.[39] Cell-free synthesis brings to convergence materials science and biomanufacturing at the nanoscale.

Biology can also combine, stack, and recombine nanostructures to produce macrostructures, such as plants and animals. Functionally graded materials differ from bulk or composite materials in that mixtures and arrangements can be deliberately adjusted within the material. The chemistries and precise spatial control required to build structurally strong, lightweight materials, or materials with corrosion resistant surfaces or embedded sensors, are difficult processes with standard chemistry and manufacturing, but perhaps possible with biological manufacturing. Our mastery of synthetic biology is likely to be key to developing a large range of such materials.

Energy Production and Management

Fundamentally, biological organisms are simply energy management systems that take in energy in the form of food and/or sunlight, perform energy conversions, and then expend or store that energy. Commercial industry (a decidedly non-biological creature) is now looking to synthetic biology to mimic some of these processes to create artificial photosynthesis, create biofuels, and develop bio-battery energy storage capabilities. Materials that can help catalyze or facilitate ion transport are important to quality batteries, and synthetic biology might generate specialized materials for applications in this domain of battery refinement.

Current capabilities use engineered *E. coli*[40] to convert waste materials (such as wastepaper and carbohydrates) or microalgae[41] harvesting the sun's energy to produce diesel fuel alternatives. While much vaunted, such technologies have, to date, attained limited commercial success. Another project is researching the use of modified DNA to encode enzymatic processes that convert complex organic fuels (likely, waste products) into energy.[42] Researchers are also very interested in harvesting solar energy through a synthetic form of photosynthesis, thus converting the sun's plentiful photons to accessible chemical or electrical energy.[43]

Artificial lighting is a major consumer of electrical energy, but can potentially be replaced by bioluminescence, enhanced using synthetic biology. Far from being a jar of fireflies, engineered luminescent microorganisms might be able to produce a "living light" efficiently and sustainably.[44]

Most of the potential uses of synthetic biology for energy production and management are in the basic research phase. A conference sponsored by the Basic Research Directorate within the Department of Defense (Research and Engineering) in 2018 explored "Future Directions of Synthetic Biology for Energy and Power," and considered basic research directions involving electrocatalysis, electron storage (batteries), and ion transport materials.[45] Each of these directions can support application areas discussed above. The workshop concluded that the applications are varied and promising, but that much development will be needed to translate the scientific principles into practical applications.

Information Technology

While there are no extant computers based on synthetic biology, it is within the realm of possibility and a logical development based on a fundamental understanding of biological principles.

This discussion is not about attempting to mimic the human brain or simulate intelligence through the workings of neurons. Instead, we look at the functions of DNA editing, protein production, and metabolite synthesis as information processing tools and consider whether the storage and logic functions that are implied by such biochemical processes could be used for information technology purposes.

DNA is highly stable due to its unique chemical structure and the double helix structure formed by Watson-Crick base-pairing. Each position within a given strand of DNA may contain any one of the four natural nucleotides, adenine, thymine, cytosine, or guanine (an alphabet which could be expanded with new nucleotide insertions). Each position within a stand, therefore, is equivalent to two bits (or more) in a traditional binary computer. DNA can thus be viewed as an extremely compact, stable long term information storage system.[46] Then, transcribing DNA to RNA and translating RNA into protein can be viewed as a readout function, using random access addressing. Yet more relevant to computing, the ability to edit individual base pairs through gene editing techniques (such as CRISPR) represents state transitions according to specific rules, which is analogous to the processing of a Turing machine. However, with DNA processing, it is possible to perform multiple operations at the same time (parallel computing), and thus, biological computers could represent an entirely different model of computation.[47]

These ideas have been codified in a subfield called computational synthetic biology (CSB) which has been called “the next big thing in data science.”[48] Companies have been forming in conjunction with investors, with early emphasis on data storage using DNA.[49] However, biology-based computer architectures might well be on the forefront.

Summary

In each of the application areas discussed above, there are practical ideas for producing products, and in many cases, nascent products being produced by companies. However, we have just begun to explore the potential applications of synthetic biology. Many new products and applications are possible. We are limited only by our current imagination and resources. We have likely not exhausted the areas of potential application here, having highlighted just six of today’s most promising categories. New categories are likely to emerge, as additional synthetic biology tools become commonplace. New and yet more precise gene editing capabilities are likely to emerge. New protein and nucleic acid building blocks might be developed. A better understanding of how the genetic code is transformed into multicellular structures can lead to new structural materials. Our ever-increasing understanding of protein structures and properties as a function of the genetic sequence make extensions beyond nature-provided substances increasingly plausible. At this point, there is more that is possible than there is knowledge about genes and protein properties.

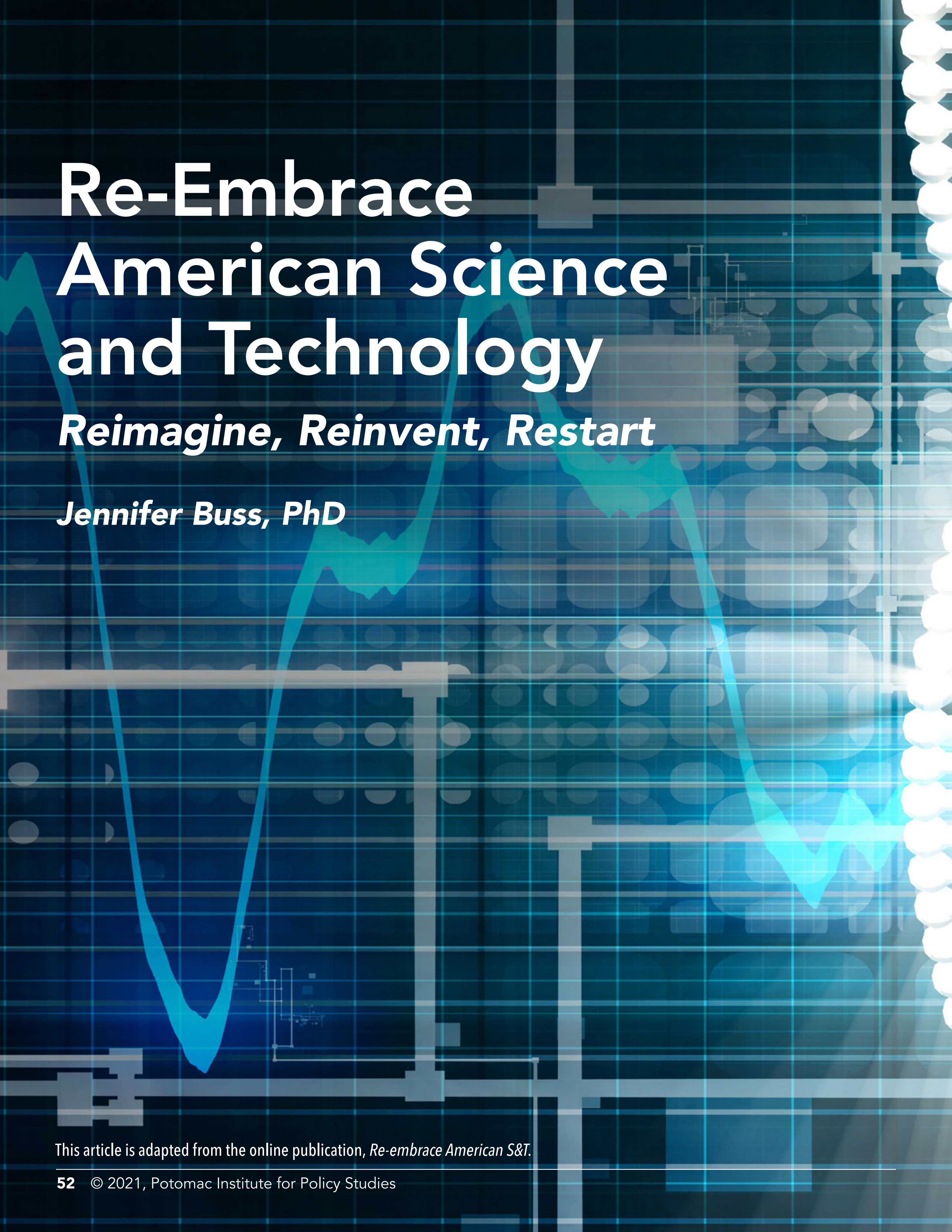
At issue is who will dominate in these fields, and who will be first to bring capabilities to market. With wide dissemination of results in basic research, as is appropriate, first to market depends on the spirit and ingenuity of entrepreneurs.

Recognizing that there are dangers, especially when unleashing reproducing biological entities, the opportunities are nonetheless compelling. The possibility of performing human gene line editing is an unfortunate distraction at this point in time, but one that will require international cooperation on responsible policies. The principal impediments to synthetic biology today consist of imagination and resources. Imagination requires a corps of educated and invested people inventing products and developing the production processes, likely as part of academia, start-ups, and government labs. Much knowledge of how to utilize synthetic biology has yet to be attained. Often, developing products will be hard, requiring a great deal of knowledge and expertise in biology and other disciplines. Such efforts ultimately require significant investment, both financially and societally as we need a cadre of scientists and entrepreneurs with sufficient knowledge to implement applications at scale. The US led the world, and reaped the benefits, in the development of microelectronics during the 20th century. It would behoove us to do the same as the burgeoning field of synthetic biology continues to emerge.

Endnotes

1. M. Jenik, et al. ,“A Programmable Dual-RNA-Guided DNA Endonuclease in Adaptive Bacterial Immunity,” *Science* (337) 2012: 816-821.
2. WalterIsaacson, *The Code Breaker* (New York: Simon & Schuster) 2021.
3. *Heritable Human Genome Editing* (Washington, DC: The National Academies Press) 2020.
4. Deborah Halber, “Nature Amplified,” Web log. *The Engine* (blog). *Medium*, December 3, 2019, https://the-engine.medium.com/nature-amplified-9fafa31b6e59.
5. Stephanie Wisner, “Synthetic Biology Investment Reached a New Record of Nearly $8 Billion in 2020 – What Does This Mean For 2021?” Synbiobeta, 2021, https://synbiobeta.com/synthetic-biology-investment-set-a-nearly-8-billion-record-in-2020-what-does-this-mean-for-2021/.
6. “Igem,” March 22, 2021, https://igem.org/Main_Page.
7. D.A. Malyshev, et al., “A Semi-Synthetic Organism With an Expanded Genetic Alphabet.” *Nature* (509) 2014: 385-388.
8. S. Hoshika, et al., “Hachimoji DNA and RNA: A Genetic System With Eight Building Blocks.” *Science* (363) 2019: 884-887.
9. “Amyris Malaria Treatment,” March 22, 2021, https://amyris.com.
10. Candice Tang, “Making Pharma Manufacturing Greener with Synthetic Biology,” Xtalks, April 8, 2019, https://xtalks.com/making-pharma-manufacturing-greener-with-synthetic-biology-1861/.
11. A.N. Miliotou and L.C. Papadopoulou, “CAR T-cell Therapy: A New Era in Cancer Immunotherapy,” *Current Pharmaceutical Biotechnology* (19) 2018: 5-18.
12. Guozhu Xie, et al, “CAR-NK Cells: A Promising Cellular Immunotherapy for Cancer,” *EBioMedicine* 59, https://doi.org/10.1016/j.ebiom.2020.102975.
13. “Synlogic Therapeutics,” April 9, 2021, https://www.synlogictx.com.
14. Kenrick Vezina, “First Fully Synthetic Organ Transplant Saves Cancer Patient,” *MIT Technology Review* July 8, 2011, https://www.technologyreview.com/2011/07/08/118144/first-fully-synthetic-organ-transplant-saves-cancer-patient/; “Tissue Engineering and Regenerative Medicine,” National Institute of Biomedical Imaging and Bioengineering, U.S. Department of Health and Human Services, April 9, 2021, https://www.nibib.nih.gov/science-education/science-topics/tissue-engineering-and-regenerative-medicine; and Amirah Al Idrus, “How Far Are We from Lab-Grown Organs? This Y Combinator Startup is Printing a Road Map,” *FierceBiotech* March 16, 2020, https://www.fiercebiotech.com/medtech/how-far-are-we-from-lab-grown-organ-transplants-y-combinator-startup-printing-a-road-map.
15. “Oisin Biotechnologies,” April 9, 2021, https://www.oisinbio.com; David Ewing Duncan, “The Next Best Version of Me: How to Live Forever,” *Wired* March 27, 2018, https://www.wired.com/story/live-forever-synthetic-human-genome/; A.S. Deller, “How Synthetic Biology Can Increase Human Longevity,” SP8CEVC. *Medium* December 4, 2020, https://medium.com/sp8cevc-8log/how-synthetic-biology-can-increase-human-longevity-939e7bd103fa.
16. H. Collins, et al., “Information Needs in the Precision Medicine Era: How Genetics Home Reference Can Help,” *Interactive Journal of Medical Research* (5) 2016, https://doi.org/10.2196/ijmr.5199.
17. Elizabeth Kolbert, “CRISPR and the Splice to Survive,” *The New Yorker* January 11, 2021, https://www.newyorker.com/magazine/2021/01/18/crispr-and-the-splice-to-survive.
18. “Keys Mosquito Project,” March 22, 2021, https://www.keysmosquitoproject.com/.

19. "TU Delft iGem 2020 Project Description," March 22, 2021, https://2020.igem.org/Team:TUDelft/Description.
20. "Allonnia," April 9, 2021. https://www.allonnia.com/; Shweta Jaiswal and Shukla Pratyoosh, "Alternative Strategies for Microbial Rem ediation of Pollutants via Synthetic Biology," *Frontiers in Microbiology* May 19, 2020, https://doi.org/10.3389/fmicb.2020.00808. Nicholas S. McCarty and Rodrigo Ledesma-Amaro, "Synthetic Biology Tools to Engineer Microbial Communities for Biotechnology.," *Trends in Biotechnology* (37) 2019:181-197.
21. Nisha Mohanan, et al, "Microbial and Enzymatic Degradation of Synthetic Plastics," *Frontiers in Microbiology* November 26, 2020, https://doi.org/10.3389/fmicb.2020.580709.
22. Marc-Sven Roell and Matias D. Zurbriggen, "The Impact of Synthetic Biology for Future Agriculture and Nutrition," *Current Opinion in Biotechnology* 61: 102-109.
23. Marianna Limas, "Exploring Solutions To Climate Change With Synthetic Biology" *Synbiobeta* December 19, 2019, https://synbiobeta.com/exploring-solutions-to-climate-change-with-synthetic-biology/.
24. S. Belkin, et al. ,"Remote Detection Of Buried Landmines Using A Bacterial Sensor." *Nat. Biotech* (35) 2017: 308-310.
25. Ed Regis and George Church, *Regenisis* (New York: Basic Books) 2012; and "Revive & Restore – The Wooly Mammoth Project," April 8, 2021, https://reviverestore.org/projects/woolly-mammoth/.
26. "Bayer Crop Science," April, 9, 2021, https://www.cropscience.bayer.com; "Corteva Agriscience," April 9, 2021, https://www.corteva.com; "Syngenta Global," April 9, 2021, https://www.syngenta.com/en; and "BASF," April 9, 2021, https://agriculture.basf.com/us/en.html; and "Pioneer," April 9, 2021, https://www.pioneer.com/us.
27. "Pivot Bio," April 8, 2021, https://www.pivotbio.com/.
28. "Conagen," March 22, 2021, https://conagen.com/.
29. "KnipBio," April 8, 2021, https://www.knipbio.com.
30. ElieDolgin, "Will Cell-Based Meat Ever be a Dinner Staple?" *Nature* December 9,2020, https://www.nature.com/articles/d41586-020-03448-1.
31. Damian Carrington, "No-Kill, Lab-Grown Meat to Go on Sale for First Time," *The Guardian* December 2, 2020, https://www.theguardian.com/environment/2020/dec/02/no-kill-lab-grown-meat-to-go-on-sale-for-first-time.
32. "University of Michigan iGem 2019 Project Description," March 22, 2021, https://2019.igem.org/Team:Michigan.
33. "BioMason," March 22, 2021, https://www.biomason.com/.
34. Hashwardhan Poddar, et al.,"Towards Engineering and Production of Artificial Spider Silk Using Tools of Synthetic Biology." *Engineering Biology* (4) https://doi.org/10.1049/enb.2019.0017; and "Bolt Threads," April 8, 2021, https://boltthreads.com/technology/microsilk/.
35. Brooke Roberts-Islam, "Could This Innovation Be an Answer To Fashion's Plastic Problem?," *Forbes* November 30, 2020, https://www.forbes.com/sites/brookerobertsislam/2020/11/30/could-this-innovation-be-an-answer-to-fashions-plastic-problem/?sh=74e828946042.
36. "BioMADE," March 22, 2021, https://www.biomade.org/.
37. ArturoCasini, et al., "A Pressure Test to Make 10 Molecules in 90 Days: External Evaluation of Methods to Engineer Biology," *Journal of the American Chemical Society* (140) 2018: 4302-4316. Note that the researchers were successful in manufacture six of the ten challenge small molecules.
38. Hershewe, J; Kightlinger, W; Jewett, MC. "Cell-free Systems For Accelerating Glycoprotein Expression and Biomanufacturing," *Journal of Industrial Microbiology and Biotechnology* (47): 977–991.
39. R.J.R. Kelwick, et al., "Biological Materials: The Next Frontier for Cell-Free Synthetic Biology." *Front. Bioeng. Biotechnol* May, 12 2020, https://doi.org/10.3389/fbioe.2020.00399.
40. "Engineering E. coli for Biofuel, Bioproduct Production," Biological and Environmental Research, Department of Energy, June 30, 2016. https://www.energy.gov/science/ber/articles/engineering-e-coli-biofuel-bioproduct-production.
41. Chris Lo, "Algal Biofuel: The Long Road to Commercial Viability," Power Technology, January 28, 2020, https://www.power-technology.com/features/algal-biofuels-challenges-opportunities/.
42. Stephe Kuper, "US Office of Naval Research Global uses DNA to Overcome Limitations Of Portable Power Supply," *Defence Connect* June, 19 2020, www.defenceconnect.com.au/key-enablers/6299-us-office-of-naval-research-uses-dna-to-overcome-limitations-of-portable-power-supply.
43. Jeremy Shears, "Is There A Role For Synthetic Biology In Addressing The Transition To A New Low-Carbon Energy System?," *Microbial Biotechnology* (12) 2019: 824-827.
44. "Glowee," March 22, 2021, https://www.glowee.eu/.
45. Michael C.Jewett, et al., *In Future Directions of Synthetic Biology for Energy & Power*, Virginia Tech Applied Research Corporation, April 9 ,2021, https://basicresearch.defense.gov/Portals/61/Documents/future-directions/12.14.18%20FDW%20on%20Synthetic%20Biology%20for%20Energy_Power_added%20refs.pdf?ver=2018-12-14-114338-257.
46. "The Future of DNA Data Storage," (Arlington, VA: Potomac Institute for Policy Studies) 2018, https://potomacinstitute.org/images/studies/Future_of_DNA_Data_Storage.pdf.
47. Lewis Grozinger, et al., "Pathways to Cellular Supremacy in Biocomputing," *Nature Communications* (10), https://www.nature.com/articles/s41467-019-13232-z.
48. William Vorhies, "The Next Big Thing in Data Science Is …. Biology," Data Science Central (blog), June 19, 2018, https://www.datasciencecentral.com/profiles/blogs/the-next-big-thing-in-data-science-is-biology.
49. Sarah Vitak, "Technology Alliance Boosts Efforts to Store Data in DNA," *Nature* March 3, 2021, https://doi.org/10.1038/d41586-021-00534-w.



Re-Embrace American Science and Technology

Reimagine, Reinvent, Restart

Jennifer Buss, PhD

This article is adapted from the online publication, *Re-embrace American S&T*.

America must invest in bold, imaginative, and inspirational endeavors to tackle the hardest challenges facing the world–challenges which may only be overcome through inspired scientific research and inventive technological development. As Americans begin emerging from the pandemic's long shadow, we look to the future and find ourselves at a unique crossroads. Congress and the Biden administration are considering massive infrastructure investments, economic stimuli, and funding for science and technology—programs on a scale not seen in nearly 100 years. The dramatic scale of these programs necessitates that we ask ourselves the following: How can we best leverage these investments to promote American interests, retain America's leadership of the science and technology enterprise, and ensure the nation's safety, security, and prosperity for years to come? The answer is to re-embrace American science and technology.

Inspire, Inform, and Re-imagine to Promote American Science and Technology

We must apply science and technology leadership to all aspects of American life. We must inspire talented people to continue the American tradition of innovation, ingenuity, and scientific advancement. A prerequisite to maintaining global leadership in science and technology is public support for the scientific enterprise. Generations of Americans, scientists, engineers, and informed citizens alike, were inspired by 20th century scientific accomplishments—the space race, the introduction of microelectronics and personal computers, and the challenges brought on by Cold War era defense research projects. But today, it seems that reverence has waned. Distrust of scientifically enabled advancements has spiked, and public support for such investments, particularly in fundamental research, has diminished.

It is now time to dream big, to think boldly, and to inspire society through the benefits of scientific and technological leadership. America should once again tackle grand, transformative challenges such as re-imagining the International Space Station as a cooperative International Lunar Habitat, re-envisioning transportation technologies (both personal and commercial) via smart infrastructure and autonomous vehicles, and revolutionize manufacturing with programmable and biological manufacturing techniques, sustainable materials, and recycling. These are not small objectives, but they are possible. They will demand new discoveries, bring forth new products and market sectors, and stimulate a dynamic American economy. Most importantly of all, they will inspire the most talented people in the world to join together in the American science and technology enterprise.

Rebuild the Infrastructure for American Education

The United States has long enjoyed its place at the head of the global science and technology community. With the best universities and research laboratories, along with innovative industries that rapidly adapted and adopted new technologies, the United States leads the world in science Nobel prizes and remains the place for international students to come study, as well as for scientists around the world to reach the pinnacle of their career.

Continued American leadership in science and technology, however, is not guaranteed. Rivals to American dominance have observed the advantages of indigenous technological advances and have invested in long-range plans to attain excellence in science and technology across broad ranges of disciplines. US graduates in science are finding opportunities elsewhere, and American enthusiasm for science and technology has faded.

It is vital to restore American leadership in science and technology; to attract the best scientists, both domestically and internationally; to provide the best national security technologies; and to grow the economy with world leading products and capabilities. Re-invigorating American leadership in science and technology is possible because of the legacy of talent and resources still in existence. However, continued leadership requires a ready supply of scientists and technologists fed by a vibrant pipeline of training and engagement as well as protection of the intellectual property rights of the final product around the globe. The infrastructure for American science and technology includes education, training, institutions, jobs, and laboratories. In the same way that the American infrastructure of roads and bridges requires attention, the infrastructure for the American science and technology enterprise needs commitment and investment.

Capitalize on Biotechnology Advances to Remake Health Care

New technologies all around us are changing the way that we live. Changing the way we live will, naturally, change the way we provide our health care, too. Sensors, data analytics, and telemedicine are redefining 21st century health care.

Major biotechnology breakthroughs, many achieved in part due to necessity during the coronavirus pandemic, should be leveraged to provide other health benefits and redress long standing challenges such as the seasonal flu or perhaps even the common cold. Advanced sensors, wearables, and biometric data should inform doctors—not just individuals—and improve the care, and ultimately health of every American. We should continue to capitalize on the positive transformations to health care delivery as a result of the pandemic. Telemedicine should enable those in rural communities, juggling unpredictable work schedules in the gig economy, among other challenging scenarios, to receive the same high level of care enjoyed by millions of urban-dwelling Americans. Changing how we use technology changes the way we care for people and can aid in improving the lives of all Americans.

Due to its breadth and numerous applications, biotechnology research is conducted across multiple agencies in the US government. To build on recent advances, new and bold research projects and organizational structures should be promoted. Rapid progress is expected, and American leadership is required.

Leverage Science and Technology to Reduce the Greatest Risks Confronting Society

US science and technology is a lynchpin of our national security. The nation faces many threats, both natural and adversarial, a selection of which are enumerated in the Intelligence Community's 2021 Worldwide Threat Assessment. Each of these threats, among others, present daunting challenges. But we can still have faith that the American intellect can confront, mitigate, and/or deal with these serious threats. That science and technology in conjunction with sound policy, diplomacy, and good practices can prevail. But again, we must think boldly, because mitigating these threats will often necessitate defending all of humanity.

Scientists need to develop technological solutions wherever possible, balancing short-term and long-term objectives with levels of acceptable risk. We need wise resource allocation based on a sensible prioritization and risk analysis. Leveraging international collaborations is worthwhile but needs to be handled carefully to avoid assisting adversaries against our interests. Management of the options is as hard as the development of ideas to explore. But the opportunity is to utilize our demonstrated excellence in science and technology to develop defenses against the most likely threats. The key is to both develop technological solutions whenever possible, and to balance long-term with short-term approaches.

We believe the United States should focus on scientific and technological means to perform data analytics at pace with events and improve situational awareness in a world awash with information; to promote cognitive security in the face of growing algorithmic warfare; to provide clean, reliable energy supplies; and to clean the atmosphere and combat global climate change through geoengineering.

Conclusion

The continuation of America's preeminence rests on the promise of America's minds and the might, both economic and military, that they produce through scientific research and technological adaptation. We live in a complex, competitive, and technical world, therefore the United States must re-imagine and re-invent its path forward by re-embracing American science and technology.

For Further Reading

"Re-embrace American S&T: Reimagine, Reinvent, Restart," Potomac Institute for Policy Studies, February, 2021. https://potomacinstitute.org/images/studies/RE-EMBRACE_AMERICAN_S&T.pdf.

Autonomous Vehicles: What's the Deal?

Robert Hummel, PhD

Autonomous vehicle technology promises to make driverless vehicles a reality. Yet the introduction of commercial driverless vehicles has been delayed, and there are warning signals that perhaps the technology will not be ready any time soon. We list some of the warnings, successes to date, and challenges to their introduction and integration into the transportation enterprise. We note some particular special cases where introduction might be possible in the short term. One difficulty is that the development of autonomous vehicle technology is proceeding under the assumption that the infrastructure (the roads, and other vehicles) will provide minimal assistance. We note that government could accelerate the development by providing standards, sensors, and communications as part of the infrastructure as improvements are made to roads and bridges.

Disillusionment?

Very few years ago, autonomous vehicles were going to change the world. Now, it seems as though the revolution has been postponed. Indeed, in the past year, there have been significant signs that disillusionment has set in. And yet, progress continues to be made and many demonstrations and experiments show promising results. Research and development are absorbing resources and talent worldwide. Does government have a role? Where do we go from here?

Before we describe the accomplishments to date, consider the warning signals:

- Uber, which had invested billions into developing driverless vehicles for their ridesharing services (which would then become robo-taxi services), spun off its autonomous vehicle effort in late 2020 to form a new company called Aurora.[1] Uber invested $400M in Aurora.

- Lyft followed suit, selling its autonomous vehicle subdivision to a subsidiary of Toyota, in early 2021.[2] It seems that both Uber and Lyft had been competing in development of robo-taxi capabilities but became disillusioned by the delays and cost of development.

- Yandex, a Russian/Dutch concern that was (among other things) pursuing self-driving vehicles for robo-taxi services, spun off the division to an independent entity called Yanex Self Driving Group, in late 2020.[3] Independence facilitates raising venture capital.

- In 2018, prior to Uber's divestiture, an autonomous Uber test vehicle with a safety driver struck and killed a woman walking her bike across a busy highway in the dark of night.

- Waymo, a division of Alphabet, announced the departure of the CEO and many of its top executives in early 2021,[4] thereby suggesting Google's multi-year foray into the development of autonomous vehicles is also not proceeding at the expected pace.

- A preliminary investigation of an accident where a Tesla vehicle ran into a tree killing two occupants indicated that there was no one in the driver seat.[5] Tesla vehicles include an "Autopilot" mode that serves as a driver assistance system. Tesla CEO, Elon Musk,[6] denied that Autopilot was enabled at the time of the crash.

- In 2019, Phys.org provided five reasons why experts say that self-driving vehicles carrying passengers are at least ten years, or maybe multiple decades, away.[7]

- A *New York Times* article in May 2021 quotes industry executives to suggest that the "transformation" will occur over the next "30 years."[8]

No one is giving up, and none of these signals indicate that self-driving vehicles are impossible. On the contrary, many companies continue impressive research and development, and commercial success seems imminent. However, initial progress has been slower than once anticipated.

Positive Autonomous Vehicle Developments

Plenty of experimental systems operate on real roadways, carrying human occupants. In some cases, the vehicle operates without a safety driver. All the major automobile companies either have R&D efforts in subdivisions or partnerships in technology companies, or both, to develop increasingly more autonomous control systems. Moreover, some cities employ "robo-taxi" services as pilot programs.

Several technology companies have impressive demonstrations with online videos showing driverless vehicle operation. Much of the impetus is to provide and expand robo-taxi services, where the control system allows the vehicle to serve as a driverless taxi service, taking paying customers from one location to another. Much like Uber and Lyft, the service is summoned using an app.

One of the main pilot programs is taking place in Phoenix, Arizona. Google started an autonomous vehicle subsidiary in 2009, which is now part of the Alphabet portfolio in a company called Waymo.[9] Waymo One, out of Phoenix, is an autonomous vehicle ridesharing service that operates without people in the driver's seat.[10] Waymo Driver is their autonomous driver technology, which they claim is the world's most experienced driver according to odometer readings.

Other tests and pilot projects are taking place in Gangzhou, China. This large metropolitan city (the third largest city in China, 75 miles from Hong Kong) hosts a (free) robo-taxi service by WeRide,[11] with over a hundred thousand rides through 2020.[12] In addition to Gangzhou, WeRide is authorized to test driverless vehicles in San Jose and claims over 2.5 million miles of testing and operation. Another competitor in Gangzhou, DiDi Autonomous Driving,[13] is a break-out from DiDi Chuxing automaker and has raised a billion dollars equivalent in venture capital. They have an online demo of an autonomous vehicle operating for five hours without intervention from a human driver (i.e., without a disengagement).[14]

Another impressive demonstration is presented by Mobileye, a company owned by Intel, with demonstrations of autonomous driving using visual sensing and crowd-sourced mapping technology in Jerusalem, Israel, driving for twenty minutes in a complex urban environment without disengagements.[15] The vehicle merges into traffic, navigates complex turns, and senses and avoids pedestrians.

One of the main autonomous vehicles companies, Cruise,[16] is a subsidiary of GM and is backed by GM and Honda, with further investments from Microsoft, Walmart, and venture capital. Cruise has a resulting valuation of at least $30 billion.[17,18] They have displayed a driverless concept car called Origin, which has no steering wheel or gas pedal. Intended ultimately for the ridesharing market, it is likely to initially see use in special transport situations, like transporting people from parking lots to tourist venues. (A French company, EasyMile, has fielded such driverless shuttles.[19]) Cruise has been testing autonomous vehicles based on the Chevy Bolt in San Francisco and claims to have logged the most miles compared to all competitors.[20] These tests are said to be driverless with minimal intervention by a safety driver (said to be Society of Automotive Engineers [SAE] Level 4 conditions).[21] In March 2021, Cruise acquired Voyage—a company that has tested some of its autonomous vehicle technology under certain speed restrictions within retirement communities.[22] Cruise has plans to start a robo-taxi service in Dubai in 2023.[23]

There are dozens of other technology companies developing autonomous vehicle components or supporting technologies. Inexpensive sensors and communications devices are especially important. Much development is required to train (or teach) systems about special cases in navigation and traffic negotiation.

All of this implies that the autonomous vehicle revolution is about to happen, with commercial availability for driverless vehicles and robo-taxi services imminent. However, the tests to date all have certain restrictions and constraints, with the hope that these restrictions can be overcome through further development. Moreover, most of the development assumes that the road and associated infrastructure is unavailable to assist autonomous vehicles, except that GPS and geolocation services are a given. Because the challenges are great, assistance from infrastructure could be important to safety and further success.

Challenges

Car and Driver says that R&D for self-driving cars has cost $16B as of early 2020, and there is not much short-term reward.[24] A significant fraction of the US total R&D budget is dedicated to the development of various forms of autonomous vehicles, largely funded by venture capital. The opportunity costs are significant, but the potential payoff is large. So far, the payoff is minimal in terms of return on investment.

Still, the demos and testing of the companies engaged in developing autonomous vehicles continue to show steady progress and impressive results. We noted commercial robo-taxi services in Phoenix and Gangzhou, and we expect to see them elsewhere, soon. Yet the warning signs and experts suggested that long-term benefits might be decades in the future. So, what is the disconnect? Will we see driverless vehicles in everyday traffic soon? Will robo-taxis become the more common form of commuting, and when?

The difficulty is that there are important challenges to the widespread adoption of truly autonomous, driverless vehicles.

Most of the time when driving, a person pays relatively little attention, adjusting the steering or acceleration in response to simple visual inputs. Machine learning can accomplish the same by interpolating from training data to provide safe autonomous navigation of a vehicle, for those cases where there is plenty of data. The methods can include a mix of deep neural networks, together with rules based on specific inputs like lane markers and stop signs. And thus, driverless vehicles have shown a level of success, generally with a safety driver present, in limited domains.

But problems arise when you consider the volume of activity that is encompassed by vehicular transport in the United States. Americans drove around 3.2 trillion miles in 2019 (fewer miles were driven during the 2020 pandemic).[25] In 2020, all autonomous vehicles world-wide drove less than 2 million miles, which was more than in 2019.[26] The leaders (by far) in miles driven were Waymo and Cruise. While 2 million miles is sufficient to start to give an indication of the frequency in which an operator needs to take over (disengagements), it can't possibly be representative of all the various conditions and situations that are encountered in 3.2 trillion miles. Waymo says that they have driven a total of 20 million miles since 2009[27] (a twelve-year period), with 6.1 million of those miles in the Phoenix, Arizona metropolitan area.

While millions of miles have been accumulated for training, trillions of miles will be necessary. That is six orders of magnitude apart. Thus, the challenge is to deal with many kinds of weather conditions, environments, and navigation situations to include parking lots, tunnels, underground facilities, round-abouts, etc. Simulations can fill in needed experience to a degree, but massive collection from non-autonomous vehicles may be essential. Furthermore, statistical approaches based purely on training are likely to be inadequate: rules and methods of inference will likely need to supplement training. And then there are the extremely unusual situations.

At times, driving requires anticipation and/or analysis of the intentions of other drivers. Sometimes driving requires extrapolation from prior experience concerning road conditions or the local environment, with analysis based on very few, if any, prior experiences. Pre-encoded rules do not necessarily cover all possible cases. Today, machine learning techniques in artificial intelligence are not capable of such deeper reasoning and instead rely on many examples for interpolation from training data.[28] Accordingly, until artificial intelligence approaches can perform extrapolative analysis based on few or no prior experience to cause a vehicle to successfully navigate unusual or challenging situations, a fully autonomous vehicle will not be possible. On the other hand, vehicles should be able to navigate safely under many conditions when these rare situations are not present.

There is also the issue of autonomous vehicles operating in conjunction with human drivers. Humans infer the intentions of other drivers all the time to ensure their own safety. They might have difficulty inferring the intentions of autonomous vehicles, and autonomous vehicles almost certainly are not good at inferring humans' intentions as it bases its decisions on average cases.

It is widely thought that once autonomous vehicles are safer than human drivers, autonomous vehicles will find a widespread commercial market. The economic benefits are large, providing the driver can be taken out of the loop. But safety is a separate issue. The marketplace not only needs to *know* that autonomous vehicles are safe, but they also need to be *convinced*.

Beyond statistical significance in proving safety, convincing consumers might require that autonomous vehicles be vastly safer than human drivers. The average person overestimates their own abilities, but also assumes a greater risk of loss when emplacing trust in someone else, or something else.

One of the greatest challenges, however, will be liability. Currently, drivers pay insurance companies to pay for losses, because drivers incur the liability for most accidents. With autonomous vehicles, the software developers must incur at least some of the liability, which will significantly raise the cost of software delivery and thus the cost of the vehicles. While overall costs might simply be shifted, or even decreased, the perceived entry cost of possessing an autonomous vehicle, or using a robo-taxi, might inhibit adoption.

Prognosis

First, note that advanced driver assistance systems (ADASs) have already made driving far safer and have begun to dominate the market for new cars. While far from driverless technology, these systems use sensors and processing to assist drivers in keeping vehicles and their occupants safe. But ADASs do not get rid of the driver, and thus the payoff is in terms of safety. We expect increasing sophistication of available commercial ADASs.

Greater levels of autonomy are possible, but there remain issues around highly unusual situations and conditions which currently require the cognitive skills of a thinking human driver. The goal, for the time being, will therefore be to develop vehicles in which a human can take charge when required, but most of the time offer minimal input. Safety will be enhanced, and drivers will have more freedom if they can be divested from the mundane driving tasks. However, for now, having a driver (whether in the vehicle or remote) that can take over at a moment's notice will remain essential.

Personal and commercial vehicles can minimize the amount of time in which a driver needs to take control by making use of a smart road and communications that integrates local data from multiple vehicles, environment conditions, and road sensors. Integration of the information from the multiple vehicles in a local vicinity can enhance both safety and efficient flow. A logical component of a hybrid approach to autonomous or semi-autonomous vehicles includes smart road infrastructure.

Based on the successful demonstrations and ongoing experimental services, there are likely certain applications that might provide commercial payoffs for mostly autonomous vehicles.

Robo-taxi services in limited areas: Most taxi and ride-sharing services operate in limited urban areas, taking passengers from one easily accessible location to another. By learning the precise layout of roads in a region of a few square miles, or even a few hundred square miles, and the rules of the road for that limited area, a large proportion of rides might be accommodated in a driverless fashion. This remains the hope, and while the challenges include operating in a hybrid environment with non-autonomous vehicles and pedestrians, robo-taxi services in specific regions are likely viable, especially if smart infrastructure can assist the vehicles. There will likely be certain limitations, like fixed pick-up locations, as in current pilot projects, but the economic drivers are compelling.

Interstate portal to portal cargo delivery: Trucking can be transformed by using driverless vehicle technology to move trucks from one portal along a major long-haul artery (like an interstate highway) to another point "down the road," so that a driver can deliver the truck from a complex urban location to the portal, and a different driver distributes the cargo by picking up the truck at the second portal.[29]

Full autonomous mode: ADAS systems might become so sufficiently trustworthy that a driver can allow the vehicle to go into a super-cruise control mode, for example on an interstate that does not require the driver to pay attention until alerted and given sufficient warning that human control will be required.

Delivery of packages: Driverless package delivery services might be viable for certain sets of distribution points and in certain areas. Expanded use of bike lanes and dedicated lanes might help smooth delivery of goods.

How Government Can Help

Government's primary role is to enhance safety of vehicular traffic. Safety is greatly improved by incorporating ADASs into most new vehicles and also by improvements to the infrastructure. Safety is also enhanced if that infrastructure can promote sharing of data among vehicles and with the road, i.e., smart roads. While we wait for breakthroughs that allow for greater full autonomy that can take the human out of the loop entirely, it behooves all stakeholders to pursue dual paths that utilize advanced driver assistance as well as novel and advanced smart road technologies, including high bandwidth communications and fast processor speeds to assist in navigating and controlling traffic.

Fully autonomous vehicles, as indicated by SAE autonomy levels 4 and 5, could accrue major economic benefits and so are desirable to help grow the economy and improve standards of living. However, assuming that their introduction is imminent is not an excuse to neglect infrastructure improvements that enhance safety, irrespective of the level at which the vehicles perform. In fact, we cannot be sure that full autonomy is imminent or at what cost (monetarily or in terms of safety) it might be acquired. In any case, smart road technology can enhance both safety and driverless vehicle introduction, working in conjunction with autonomous vehicle technology hosted entirely on the vehicle.

The task of installing appropriate infrastructure for smart roads is daunting and yet can happen incrementally, as the infrastructure for roads and bridges are renewed. There are multiple models for how industry can team with government to establish the technological infrastructure to help guide vehicles safely and efficiently; indeed, this already exists with respect to traffic lights and existing highway sensor systems.

On an interim basis, it is possible that the interstate highways can be upgraded, such that drivers could allow vehicles to be completely autonomous from one depot or entry ramp to a destination depot or exit ramp, and that the driver pays attention in local traffic between the origin and destination and the major depot points. For long haul cargo traffic, for example, the driver could depart at the depot location and be joined by a different driver at a depot near the destination point. Of course, such transit is already commonplace using rail lines.

Accordingly, government can assist in setting standards, facilitating communications, and ensuring that road infrastructure allows modern and upgradable data collection points and data sharing capabilities. Working with industry, government can help define the application programming interfaces (APIs) and data formats that would enable roads to communicate and coordinate with multiple vehicles. China's Belt and Road Initiative (BRI) ostensibly includes smart technology that will permit China to collect massive amounts of data[30] but may also by default set standards by virtue of being the first to market. While there is much interest in smart road technology, there is insufficient action in the United States and a lack of governmental coordination that can rationalize the marketplace and guide auto manufacturers in a coherent fashion.

Government might also be able to assist in the development of autonomous vehicle technology, for example for robo-taxi services in specific cities, regions, or for certain application domains, by furthering the sharing of data and setting standards. However, it is probably not viable for government to collect data to be used to train algorithms, despite the need for massive amount of training data, due to privacy concerns. Instead, government might facilitate the formation of data collection entities that work cooperatively with smart road developers and automakers.

We may experience further advances in autonomous conveyance of cargo and passengers, or perhaps we will stall short of full autonomy and always require a human driver to be ready to take control if called upon. Either way, technological advances towards both autonomous vehicle control and smart road infrastructure can make transportation safer, more efficient, and less costly, benefiting all of society.

Acknowledgements

Dr. Hummel thanks the staff of the Potomac Institute who all contributed significantly to this document. Without the entire staff of the Potomac Institute, this document would not have been possible.

Endnotes

1. "Aurora Acquires Uber's Automated Driving Unit–And Uber's Cash," *Forbes* December 7, 2020, https://www.forbes.com/sites/samabuelsamid/2020/12/07/aurora-acquires-ubers-automated-driving-unitand-ubers-cash/?sh=4b93a95963eb.
2. Yandex Self-Driving Group, "Toyota is Buying Lyft's Autonomous Car Division For $550 Million," *The Verge* Sept. 3, 2020, https://www.theverge.com/2021/4/26/22404406/toyota-lyft-autonomous-vehicle-acquisition-amount-deal.
3. Yandex Self-Driving Group, "Yandex Self Driving Group Takes a New Leap With $150M In Investment," *Medium* Sept. 3, 2020, https://medium.com/yandex-self-driving-car/yandex-self-driving-group-takes-a-new-leap-with-150m-in-investment-8e9b86803d6a.
4. Billy Duberstein, "Is Waymo a Bust?" The Motley Fool, May 26, 2021, https://www.fool.com/investing/2021/05/26/is-waymo-a-bust/.
5. "Tesla CEO Elon Musk Responds To Texas Crash In Investigation Into Two Deaths," NBC News, https://www.nbcnews.com/news/us-news/tesla-ceo-elon-musk-responds-texas-crash-amid-probe-two-n1264623.
6. Mr. Musk's official title is Technoking of Tesla. A position from which he acts as the chief executive.
7. Five reasons experts think autonomous cars are many years away (phys.org) https://phys.org/news/2019-04-autonomous-cars-anytime.html.
8. "The Costly Pursuit of Self-Driving Cars Continues On. And On. And On.," *The New York Times* https://www.nytimes.com/2021/05/24/technology/self-driving-cars-wait.html.
9. "Waymo," https://waymo.com/.
10. "FAQ," https://waymo.com/faq/.
11. "WeRide," WeRide. https://www.weride.ai/en/dmv-unmanned-test-license-en/.
12. "WeRide Robotaxis Gain Loyal Passengers But Fixed Pick-Up, Drop-Off Spots Irk Some, Survey Shows," *South China Morning Post* https://www.scmp.com/tech/start-ups/article/3111277/weride-robotaxis-gain-loyal-passengers-fixed-pick-drop-spots-irk.
13. "Autonomous Driving-DiDi technology," DiDi official website (didiglobal.com). https://www.didiglobal.com/science/intelligent-driving.
14. "Didi Autonomous Driving to Pocket USD 300 million Investment, Raising Potential Market Value Higher Than Pony.ai," Synced, https://syncedreview.com/2021/06/01/didi-autonomous-driving-to-pocket-usd-300-million-investment-raising-potential-market-value-higher-than-pony-ai/.
15. "Autonomous Driving & ADAS (Advanced Driver Assistance Systems)," Mobileye https://www.mobileye.com/.
16. "Cruise," https://www.getcruise.com/.
17. "Walmart Investing in GM's Cruise Self-Driving Car Company," CNBC, https://www.cnbc.com/2021/04/15/walmart-investing-in-gms-cruise-self-driving-car-company.html.
18. https://millennialmoney.com/argo-ai-stock-ipo/.
19. "Fully Driverless First/Last Mile Shuttle Service on Medical Campus," EasyMile, https://easymile.com.
20. Riley Beggin and Kalea Hall, "Cruise Posted Most California AV Testing Miles in 2020," *Transport Topics* February 10, 2021, https://www.ttnews.com/articles/cruise-posted-most-california-av-testing-miles-2020.
21. Andrew J. Hawkins, "Cruise is Now Testing Fully Driverless Cars In San Francisco," *The Verge* December 9, 2020, https://www.theverge.com/2020/12/9/22165597/cruise-driverless-test-san-francisco-self-driving-level-4.
22. KirstenKorosec, "Cruise Acquires Self-Driving Startup Voyage," *TechCrunch* March 15, 2021, https://techcrunch.com/2021/03/15/cruise-acquires-self-driving-startup-voyage/.
23. https://millennialmoney.com/argo-ai-stock-ipo/.
24. "Companies Have Spent $16 Billion on Self-Driving-Car Research," Car and Driver https://www.caranddriver.com/news/a30857661/autonomous-car-self-driving-research-expensive/.
25. Alternative Fuels Data Center: Maps and Data - Annual Vehicle Miles Traveled in the United States (energy.gov) https://afdc.energy.gov/data/10315.
26. "Chart: The Self-Driving Car Companies Going The Distance" Statista, https://www.statista.com/chart/17144/test-miles-and-reportable-miles-per-disengagement/.
27. "Safety Report and Whitepapers, " Waymo, https://waymo.com/safety/.
28. See Erik J. Larson, *The Myth of AI, Why Computers Can't Think The Way We Do* (Cambridge: Bellnap Press) 2021.
29. "Moving us Towards a Self Driving Future," Aurora, https://aurora.tech/.
30. "Weaponizing the Belt and Road Initiative," Asia Society Policy Institute, September 8, 2020, https://asiasociety.org/policy-institute/weaponizing-belt-and-road-initiative.

111010101110 10101010 10 10 101010101
111010101110 10101010 10 10 101010101
111010101110 10101010 10 10 101010101
111010101110 10101010 10 10 101010101
10101010 10 10 101010101

Featured Authors

Robert Hummel, PhD

STEPS, Editor-in-Chief
Chief Scientist, Potomac Institute for Policy Studies

Dr. Robert Hummel serves as the Chief Scientist of the Potomac Institute for Policy Studies in the Science and Technology Policy Division and is a member of the Center for Revolutionary Scientific Thought. He is the author of the Potomac Institute book, *Alternative Futures for Corrosion and Degradation Research* and is also serving customers in DARPA and OSD. He is the principal author of the Institute's forthcoming book on machine intelligence. Prior to joining the Potomac Institute, he served as a program manager at DARPA for nearly nine years, managing and initiating projects in information exploitation, computer science, and sensor design. Prior to joining DARPA, he was a tenured faculty member at NYU's Courant Institute of Mathematical Sciences in the Computer Science Department, where he did research in computer vision and artificial intelligence. Dr. Hummel earned his PhD in mathematics from the University of Minnesota, and he holds a B.A., also in mathematics, from the University of Chicago.

Timothy W. Bumpus, PhD

STEPS, Associate Editor
Research Associate, Potomac Institute for Policy Studies

Dr. Timothy Bumpus received his PhD in chemical biology from Cornell University where, as a National Science Foundation Graduate Research Fellow, he designed and implemented new chemical tools to study lipid centric cell signaling processes. Prior to Cornell, Dr. Bumpus attended Luther College where he received his B.A., majoring in chemistry, biology, and mathematics. He now brings his diverse scientific expertise to bear on the many, varied science and technology policy issues facing the country as part of the Potomac Institute for Policy Studies' research staff.

Jennifer Buss, PhD

Chief Executive Officer, Potomac Institute for Policy Studies

Dr. Jennifer Buss serves as the CEO of the Potomac Institute for Policy Studies. The Institute develops meaningful science and technology policy options through discussions and forums and ensure their implementation at the intersection of business and government. She has extensive experience examining policy issues in support of NASA, and has been involved in their strategic planning processes for astronaut medical care and cancer diagnostics and therapeutics. She manages a variety of OSD programs including an outreach effort for the Department of Defense to the start-up community across the country to find innovative technologies to meet the challenges faced by the Services and Government agencies. Dr. Buss performs science and technology trends analysis and recommends policy solutions to some of the country's most pervasive problems. She has also directed and assisted research on numerous government contracts, including systematic reviews and gap analyses. Dr. Buss is an authority in her scientific field with national recognition in her area of expertise. She is responsible for major projects requiring integration/coordination across multiple scientific disciplines.

Honorable Alan R. Shaffer

Board of Regents Member, Potomac Institute for Policy Studies

The Honorable Alan R. Shaffer served as the Deputy Under Secretary of Defense for Acquisition and Sustainment (A&S) from January 2019 to January 20, 2021. Senate confirmed in January 2019, he was responsible to the Under Secretary of Defense (A&S) for all matters pertaining to acquisition; contract administration; logistics and materiel readiness; installations and environment; operational energy; chemical, biological, and nuclear weapons; the acquisition workforce; and the defense industrial base.

From 2015 to 2018, Mr. Shaffer served as the Director, NATO Collaboration Support Office in Neuilly-sur-Seine, France. In this role, he was responsible for coordinating and synchronizing the Science and Technology (S&T) collaboration between NATO member and partner Nations, comprising a network of about 5,000 scientists.

Previous to his role at NATO, Mr. Shaffer served as the Principal Deputy Assistant Secretary of Defense for Research and Engineering (ASD(R&E)) from 2007-2015. In this position, Mr. Shaffer was responsible for formulating, planning and reviewing the DoD Research, Development, Test, and Evaluation (RDT&E) programs, plans, strategy, priorities, and execution of the DoD RDT&E budget that totals roughly $25 billion per year. He also served twice as the Acting Assistant Secretary of Defense for Research and Engineering from 2007-2009 and 2012-2015.

In 2009, he was appointed as the first Director, Operational Energy, Plans and Programs (Acting). Mr. Shaffer has also served as the Executive Director for several senior DoD Task Forces, including review of all research, acquisition, and test activities during the 2005 Base Realignment and Closure. In 2007, he was the Executive Director for the DoD Energy Security Task Force and, and from 2007-2012, he served as the Executive Director of the Mine Resistant Ambush Protection (MRAP) Task Force, where he was responsible for oversight, fielding and employment of 27,000 MRAPs across the Department of Defense.

Before entering the federal government, Mr. Shaffer served 24 years as a commissioned officer in the United States Air Force and retired in the grade of Colonel. While serving, he held positions in command, weather, intelligence, and acquisition oversight with assignments in Utah, California, Ohio, Honduras, Germany, Virginia, and Nebraska.

His military career included deployments to Honduras in the mid-1980s and direct support of the United States Army, 3rd Armored Division in Hanau, Germany. During Operation DESERT STORM, he was responsible for deployment of the 500-person theater weather force and upon retirement from the Air Force in 2000, Mr. Shaffer was appointed to the Senior Executive Service. In 2001, he assumed the position as Director, Plans and Programs, Defense Research and Engineering.

Mr. Shaffer earned a Bachelor of Science in Mathematics from the University of Vermont in 1976, a second Bachelor of Science in Meteorology from the University of Utah, a Master of Science in Meteorology from the Naval Postgraduate School, and a Master of Science in National Resource Strategy from the Industrial College of the Armed Forces. He was awarded the Meritorious Executive Presidential Rank Award in 2004, the Department of Defense Distinguished Civilian Service Award, and the Distinguished Executive Presidential Rank Award in 2007 and 2015.

Alyssa Adcock, PhD

Research Fellow, Potomac Institute for Policy Studies

Dr. Alyssa Adcock is a science and technology (S&T) Policy Research Fellow. At the Institute, she has been involved with several efforts focused on providing strategic S&T recommendations and technical forecasting to government customers including ongoing work with NASA. Dr. Adcock earned her PhD from Georgetown University in Inorganic Chemistry. Her graduate research focused on bismuth and rare earth element materials to address energy, lighting, and security needs as well as uranium chemistry relevant to nuclear waste and environmental management. She received her BS in Chemistry at Jacobs University in Germany and served as an intern at the Carnegie Institute of Washington's Geophysical Laboratory focusing on origin of life and geochemistry research. Dr. Adcock is a member of the Graduate Education Advisory Board of the American Chemical Society.

Sharon Layani

Research Analyst, Potomac Institute for Policy Studies

Sharon Layani is a Research Analyst in the S&T Division. She provides assessments of emerging science and technology trends, government acquisition strategies, strategic planning, and policy recommendations. Prior to her work at the Institute, she served as Research Associate and Research Coordinator at the International Center for Terrorism Studies. Her work focused on counterterrorism, international security, and rule of law issues. She provided research support and analysis for books, such as *NATO: From Regional to Global Security Provider* (2015) and *The Islamic State: Combating a Caliphate Without Borders* (2015), and assisted on a number of counterterrorism reports and projects. Ms. Layani served on the senior staff for *Terrorism: An Electronic Journal and Knowledge Base* and coordinated foreign policy and national security-related seminars. Ms. Layani graduated from the University of Michigan with a double major in Political Science and Biopsychology, Cognition, and Neuroscience, and a minor in International Studies focusing on the Middle East.

Michael Swetnam

Founder, former CEO, and former Chairman of the Board, Potomac Institute for Policy Studies

Michael Swetnam assisted in founding the Potomac Institute for Policy Studies in 1994. Since its inception, he served as Chairman of the Board and was the Institute's Chief Executive Officer until his death in 2020.

Mr. Swetnam dedicated his life to the service of our country, spending nearly a quarter century in the U.S. Navy, both as an active and reserve officer. He then worked for the Director of Central Intelligence as a Program Monitor on the Intelligence Committee Staff. He developed and presented the National Security Agency Budget to Congress. He also helped develop, monitor, and present the DOE Intelligence Budget to Congress. From 1990-1992, Mr. Swetnam served as a Special Consultant to President George H. W. Bush's Foreign Intelligence Advisory Board. There, he provided expert advice on Intelligence Community issues and assisted in authoring the Board's assessment of Intelligence Community support to Desert Storm and Desert Shield. Before founding the Potomac Institute, Mr. Swetnam worked in the private sector as a Vice President of Engineering at the Pacific-Sierra Research Corporation, Director of Information Processing Systems at GTE, and Manager of Strategic Planning for GTE Government Systems.

Mr. Swetnam was passionate about national security. He authored and co-authored several books and edited many articles on the subject, including: Al-Qa'ida: Ten Years After 9/11 and Beyond, Cyber Terrorism and Information Warfare, and Usama bin Laden's al-Qaida: Profile of a Terrorist Network. "There have always been small groups and individuals who have threatened societies and nations around the world. The difference today is that advanced technologies, particularly the spread of advanced technologies of mass destruction are enabling these groups to threaten us in a way that, in the past, was reserved only to nation states," Swetnam once told the Nuclear Threat Initiative Project.

Mr. Swetnam also served on several boards and committees. He'd been a member of the Technical Advisory Group to the United States Senate Select Committee on Intelligence where he provided expert advice to the U.S. Senate on the research and development investment strategy of the Intelligence Community. He was also Chairman of the Term Limits Referendum Committee (1992-93); President (1993) of the Montgomery County Corporate Volunteer Council, Montgomery County Corporate Partnership for Managerial Excellence (1993); and the Maryland Business Roundtable (1993). He was on the Board of Directors of Space and Defense Systems Inc., Dragon Hawk Entertainment Inc., and the Governing Board of the Potomac Institute of New Zealand.

POTOMAC INSTITUTE FOR POLICY STUDIES

"We are not looking for incremental ways of addressing Science and Technology (S&T) challenges. We are looking for big, bold ways of addressing a new world."

MICHAEL S. SWETNAM
1952 - 2020

STEPS (Print) ISSN 2333-3219

STEPS (Online) ISSN 2333-3200

POTOMAC INSTITUTE PRESS