STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

ISSUE 10 2024

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

IN THIS ISSUE

The Wicked Problem that Confronts the US Space Force
Alden V. Munson, Jr. and Robert Hummel

Technology Opportunities for National Prosperity
Rosalie Loewen and Robert Hummel

The Detrimental US Tax Policy on Research and Development
Robert Hummel

Mitigating Algorithmic Targeting in Social Media Platforms
Kayla Dunn

Approaching Orbital Overload
Carrie Zuckerman

Government Opportunities for AI Technologies
Robert Hummel

POTOMAC INSTITUTE PRESS

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

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

All images Shutterstock.com, unless otherwise credited.

Cover image, page 33, 47: 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.

Editorial and Production Staff

Editor-in-Chief
Robert (Bob) Hummel
Email: **rhummel@potomacinstitute.org**

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

Editing + Design
Sherry Loveless
Email: **sloveless@potomacinstitute.org**

About the Potomac Institute for Policy Studies

The Potomac Institute for Policy Studies is an independent, nonpartisan, nonprofit, science and technology (S&T) policy research institute. The Institute identifies and leads discussions on key S&T and national security issues facing our society, providing an academic forum for the study of related policy issues. Based on data and evidence, we develop meaningful policy recommendations and ensure their implementation at the intersection of business and government.

STEPS

SCIENCE, TECHNOLOGY, ENGINEERING, AND POLICY STUDIES

CONTENTS

About *STEPS* . . . 3

About the Potomac Institute for Policy Studies . . . 4

From the CEO . . . 6
Jennifer Buss

From the Editor . . . 6
Robert (Bob) Hummel

THE WICKED PROBLEM THAT CONFRONTS THE US SPACE FORCE . . . 8
Alden V. Munson, Jr. and Robert Hummel

TECHNOLOGY OPPORTUNITIES FOR NATIONAL PROSPERITY . . . 20
Rosalie Loewen and Robert Hummel

THE DETRIMENTAL US TAX POLICY ON RESEARCH AND DEVELOPMENT . . . 30
Robert Hummel

MITIGATING ALGORITHMIC TARGETING IN SOCIAL MEDIA PLATFORMS . . . 38
Kayla Dunn

Essays and Short Papers . . . 46

APPROACHING ORBITAL OVERLOAD . . . 47
Carrie Zuckerman

GOVERNMENT OPPORTUNITIES FOR AI TECHNOLOGIES . . . 50
Robert Hummel

Featured Authors . . . 54

From the CEO

Jennifer Buss, PhD

Welcome to the latest issue of *STEPS*. This publication reflects the ongoing work at the Potomac Institute, addressing current science and technology policies that shape our society. These insights stem from our work with the government, ongoing programs, and dynamic discussions within the Institute. As a science and technology (S&T) policy think tank, we cultivate out-of-the box thinking, exploring challenges and solutions in depth. *STEPS* serves as a platform to document our intellectual debates and drive meaningful dialogue.

Our continued efforts span a select range of topics, from exploring the responsibilities and challenges of U.S. national security services to examining industry-specific issues and their broader policy implications. As we navigate questions around technological advancements, tax policy and regulatory needs, global competition, and strategic commercial investments, we aim to highlight areas where focused attention and innovative policy solutions can lead to positive outcomes for society.

The Potomac Institute has a longstanding interest in understanding the impacts of emerging technologies like semiconductors, space-based systems, and artificial intelligence. We continue to assess their broader effects on critical sectors, including information ecosystems and innovation frameworks. Our ongoing analysis and discussions help illuminate the intricate connections between technology, policy, and society.

Through *STEPS*, we not only present research findings but also share thought-provoking essays that open conversations on pressing science and technology issues. These pieces often spark discussions that evolve into substantive future engagements and policy recommendations for implementation at the intersection of business and government.

I encourage you to explore these articles and engage with us on the important issues they raise.

Jennifer Buss, PhD
Chief Executive Officer, Potomac Institute for Policy Studies
jbuss@potomacinstitute.org

From the Editor

Robert (Bob) Hummel, PhD

Academics love to ascribe ideas to others based on prior publications, as ideas are their currency. It is graduate students, however, who do much of the research and work. At the Potomac Institute, our ideas come from seminars, discussions, and suggestions—often from members of the Board of Regents or Fellows. Research associates, staff, and interns pursue these ideas, providing unsung support to archival publications. While my name appears on many of these publications, the ideas and work are frequently the result of collaborative efforts within the think tank environment of seminars, discussions, and research.

In this issue of *STEPS*, numerous affiliates contributed ideas, research, and critiques. As editor-in-chief, I take sole credit only for the conveyance. The Potomac Institute Press under the capable hands of Sherry Loveless and Alex Taliesen deserves much credit for the professional text and design of the issue.

This issue of *STEPS* features an article examining the challenges and responsibilities faced by the Space Force, drawing insights from collaborations with senior leaders and consultants familiar with the formation of this new military service. One article focuses attention on the complexities and possible solutions. Another article discusses the space debris problem.

Our engagement with the government on semiconductor industry issues and the CHIPS Act raised an important tax policy consideration: why research and development is not recognized as a customary and necessary corporate expenditure deductible for tax purposes. An article in this issue of *STEPS* highlights the need to reconsider this tax policy, which could have significant implications for innovation.

The Potomac Institute has a longstanding interest in the impacts of artificial intelligence (AI) technologies on social media and information dissemination. One of our Summer 2024 interns, under the guidance of our Intern Director, provides a fresh perspective of how social media companies prioritize engagement through targeted advertising and profiling. This analysis is crucial for understanding the policy implications of digital information ecosystems. It is gratifying to give a college student well-deserved publication credit in this forum, and we commend her article as first-rate.

Looking forward, the Institute is considering topics and issues the next administration, regardless of leadership, could prioritize in national science and technology investments. From AI regulation to commercial investments in space and satellite technology, the Institute has identified opportunities where industrial policy could justify strategic government investments to benefit society. One article in this issue of *STEPS* explores key technology opportunities for national investment.

Enjoy these articles, and let the discussions continue so that the ideas can translate into policy actions.

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

THE WICKED PROBLEM THAT CONFRONTS THE US SPACE FORCE

Alden V. Munson, Jr.

Member, Board of Regents, Potomac Institute for Policy Studies

Robert Hummel

Chief Scientist, Potomac Institute for Policy Studies

Abstract

It used to be that space was the ultimate high ground, safe from enemy attack. Space became the place to gather intelligence, surveil, reconnoiter enemy forces, transmit information globally, and command and control the application of force without risking incoming fire. Thus, the US military developed a national security strategy highly dependent on space assets based upon the assumption that those assets would be survivable. Today, those assumptions are no longer valid.

Myriad national security attributes are associated with aspects of US space policy and practice. The vulnerability of space assets and the competitive environment that now attends space practice, which accompanies the creation of the US Space Force, requires careful consideration of how the national defense posture can safely utilize capabilities in space. This article touches on some of the threats and issues associated with the use of space for national defense. While we do not address every issue related to developing new space capabilities, we explore several key concerns and offer recommendations on how these issues can be formulated for comprehensive study.

US SPACE FORCE "COMPETITIVE ENDURANCE"

As a military service, the newly established Space Force is responsible for controlling and defending US capabilities in space during times of conflict. The Department of the Navy controls the seas and littoral domains; the Army controls land to dominate territory; and the Air Force establishes air superiority. The Space Force must be able to defend and control space when needed and, more precisely, should be able to achieve "space superiority" over a range of extra-terrestrial dimensions.

The Space Force has developed the concept of *Competitive Endurance*, as defined by General B. Chance Salzman, the Chief of Space Operations,[1] as focal to preserving our assets in space, maintaining our ability to operate in space, and especially, using those assets for military purposes (*endurance*) by countering adversary malign capabilities (*competition*) and to prevent adversaries from being able to use space for their military purposes.

The issue, however, is how to achieve *Competitive Endurance*. The concept represents a desirable state in which the US can achieve space superiority at times of need. But this is a daunting challenge because there are new and serious threats to US space presence and superiority.[2] Transitioning from an uncontested environment to one wherein assets must be prepared for conflicts in space is a wicked problem.

The nation has faced such challenges in the past and has developed solutions to those problems. When the Soviet Union acquired nuclear weapons and the ability to deliver them, new concepts of defense were needed.[3] To counter adversaries' submarines, new detection and tracking capabilities were needed and devised.[4] When the USSR transitioned from a littoral to a missile-armed blue-water navy capable of threatening US power projection, new capabilities were needed—including in space. Countering non-state actors' ability to conduct terrorist attacks has required new techniques and doctrine.[5] Now, contested superiority in space has become the new challenge.

Procuring systems and new capabilities are part of the process of meeting this challenge. In so doing, the nation must also address and solve wicked problems to establish and sustain space superiority.

THREATS

Achieving *Competitive Endurance* is exceedingly difficult. Space is a hostile domain, not only to humans but also to satellites and machines.[6] Orbital mechanics make the locations of assets easy to predict once those assets are in stable orbits. By determining and detecting these orbits, adversaries can track and target and disrupt both commercial and national satellite systems.

Competitive Endurance includes the ability to deny adversaries the use of space in military conflicts, which implies that it is necessary to exceed the capabilities of adversaries to counter the effective use of space. Mere defense against threats is not sufficient.

Certain threats are well-understood and require responses to enable capabilities to continue in a time of conflict. Other threats are yet to be determined, as adversaries develop new systems and capabilities to counter and defeat both our current defenses and those defenses that adversaries envision we might develop. Deterrence is an important component of defense. As in other military domains, a "cat-and-mouse game" takes place,[7] but the domain presents new challenges. Simple physics helps to reveal many of these vulnerabilities.

For example, one pernicious threat is anti-satellite missiles that can kinetically kill existing satellites. There have been test examples of such intercepts,[8] where an interceptor takes out a satellite as a demonstration (usually a defunct satellite owned by the attacker), creating a debris field (consisting of pieces of the satellite and the interceptor). An orbital debris field can have disastrous consequences for years, if not decades, to follow.[9] The Space Force is rightly focused on defending and deterring such outcomes, whether they occur during demonstration tests or as hostilities.

Other threats to existing satellites are well known to military planners.[10] Our national assets could be physically damaged by adversary satellites that rendezvous and use grappling hooks or robotic arms to damage critical components such as antennas or solar cell panels.[11] An adversary's satellite could swallow or encase a target satellite.[12] A satellite could attach a booster to "throw" a satellite, causing it to deorbit or to be ejected into a different orbit.[13] Satellites can literally fight in space.

Further, at short distances, a satellite could jam communications with another satellite using radio frequency emissions. From a greater distance, a satellite could disable a satellite's onboard electronics through a high-power microwave attack or a directed laser beam, for example to disable optics or disrupt solar cells. Attacks, from a distance, might be used to eliminate a collection of satellites in the vicinity, depending on the amount of energy the attacking entity can emit using a single charge. An ability to generate and store large amounts of energy, along with the consequential heat, are part of the problem set, but these issues are surmountable for a determined attacker. Even more concerning is the possibility that an attacker might use a small nuclear weapon to generate an electromagnetic pulse to destroy all nearby satellites.

Attacks on space assets from the ground are also possible. For example, ground-based laser beams can use adaptive optics to focus on an adversary's satellite,[14] or use a focused electronic beam to jam or damage an orbiting satellite. Internal satellite components procured from global supply chains might have elements that allow an adversary to access, disarm, or control the satellite from the ground.

Attacks on the physical satellite are not the only vulnerability. Satellite electronics can be hacked from the ground and controlled by an adversary sending malicious instructions.[15] Ground stations might be attacked using nearby jamming signals, rendering them unable to control the satellites to which they are tasked.[16] Ground stations can also be compromised physically or through cyberattack.

The US military and many of our space assets are highly dependent on the GPS, which currently consists of 31 satellites, 6 of which are the most recent Block III satellites with improved defenses against jamming and interference.[17] However, if a fraction of these satellites were to become disabled, both military space assets and many civilian systems would become incapacitated.[18] It is not just terrestrial ground navigation systems that are at risk. Satellite-to-satellite communications rely on the precise location of each and every satellite in their constellation, and today, that reliance depends on GPS. Worryingly, it is not an extreme challenge to jam or spoof GPS from the ground or space,[19] partly because the current system is deliberately "open" during normal operations.[20] There is an ongoing program to make jam-resistant receivers with special robust modes of operations available to military and civilian users, but this effort requires retrofitting existing platforms.[21]

Technological solutions exist for each of these known attack vectors; however, defenses must be integrated into new designs, and ambitious retrofits might be necessary. More often, replacements for existing satellites will need to be fielded. There may be attack vectors that have not yet been considered.

Even before the creation of the Space Force in 2019, a new strategic threat confronted the military in the form of "hypersonic weapons."[22] Responsibility for detecting, tracking, intercepting, and defending against these weapons must be coordinated among the Space Development Agency and Space Systems Command (both part of the Space Force), the Missile Defense Agency, and DARPA efforts in operationally relevant research projects.[23]

A novel threat is posed by hypersonic glide vehicles (HGVs), developed and tested by both Russia and China.[24] The speed of these weapons is much greater than that of a conventional cruise missile. However, their most important characteristic is that they are maneuverable during fly-out. HGVs operate in the Earth's upper atmosphere, where they use the atmosphere to fly aerodynamically and are only visible from the ground for a few hundred miles. These vehicles can be intercontinental and are presumed to be very accurate at hitting their target. By ascending higher, they can enter an orbital phase, thereby becoming a hybrid atmospheric and fractional orbital bombardment system (FOBS)[25] with nearly unlimited range. Russia developed FOBS in the 1960s as nuclear weapon delivery systems, which were later prohibited by the SALT II treaty.[26]

Hypersonic glide vehicles and related developments change the strategic calculus, not the least because the target of an attacking missile cannot be discerned from its ballistic path soon after launch. Rather, they need to be detected and tracked from above because installing enough ground radars is not practical. HGVs are small and difficult to detect, track, and distinguish from decoys. They can be used tactically, for example, against ships at sea,[27] and could be used in numbers to attack a target from multiple directions. They have been designed to deliberately circumvent many systems the US has developed to defend against strategic threats.[28] Thus, the cat-and-mouse game continues.

Taken together, the developments and threats by adversaries pose a significant challenge in establishing *Competitive Endurance* for space. Additionally, it poses a challenge to the US Department of Defense to establish military dominance and credible deterrents, recognizing that space is increasingly important to the military and that intercontinental high-altitude maneuverable precision weapons require new defenses.

In some ways, this situation is similar to the challenges that the nation faced when the Soviet Union acquired nuclear weapons. These new challenges may seem less daunting, but one can argue that the cumulative new challenges present a more complex situation, given that the threats are equally as consequential to those faced during the Cold War. The challenges require solutions.

POSSIBLE SOLUTIONS

There are point solutions to many of these individual vulnerabilities. For example, the electronics in a satellite system vulnerable to attack by high-power microwaves can be replaced by a spare unit that is shunted into place after damage to the primary system. A grappling hook attack can be countered by a "battle bots" contest that fends off or disturbs the orbit of an attacking satellite. An optical system that is vulnerable to a laser attack can use an electronic shutter. Satellites can use thrusters to modify their orbits (albeit at the expense of fuel), maneuvering in space to defeat attacks that make use of their predictable orbits. Legacy systems might be retrofitted with bolt-on packs that permit maneuverability.

GPS satellites are in medium earth orbit at about 20,000 kilometers altitude. This renders them safer than low earth orbit satellites. The threat of an adversary satellite in proximity would be easily detected. Maneuverability of the GPS satellites would be technically challenging (for receivers, but not impossible). The latest GPS block upgrades have higher power and backup modes to counter jamming and other threats.[29] GPS satellites might be reconstituted quickly if there are sufficient spares and rapid launch accessibility. There are alternative methods of geolocation (terrestrially as well as in orbit), so reliance on GPS can be avoided by adopting entirely new location services.

Defending against hypersonic vehicle capabilities is more challenging, but the Space Development Agency (SDA) is now developing detection and tracking systems,[30] and the Missile Defense Agency's Ground Based Interceptor program is developing ground-based terminal interceptors.[31]

The primary defense mechanism being contemplated entails the use of "proliferated" satellite architectures, usually in low earth orbit, to accomplish tasks that might otherwise use relatively few, larger, and more vulnerable assets. Each satellite in a proliferated constellation remains individually vulnerable. Still, it would be difficult for an adversary to quickly disable a large portion of a constellation consisting of hundreds (or thousands) of individual satellites. SDA's constellation is intended to consist of over 1,000 satellites that are replenished regularly.[32] Other national capabilities, such as surveillance from space, could also be replaced or augmented with proliferated architectures to enable greater system resilience. In some cases, the transition to a proliferated architecture of (smaller, simpler) satellites trades some decrement in functional quality for enhanced safety in numbers.

Commercial companies are also developing distributed architectures of satellites. Communication capabilities involving thousands of satellites are already in place with *SpaceX*'s Starlink system; and *Amazon*'s Project Kuiper is expected to field thousands of small satellites.[33] *Planet* currently operates over 150 small satellites capable of five-meter resolution imaging, and other companies have small constellations of surveillance satellites, including those with synthetic aperture radar and infrared imaging capabilities.[34] *Hawkeye 360* operates nine clusters of three satellites each to perform triangulated geolocation of RF emitters (e.g., for maritime vessel tracking).[35] The Space Force must decide if commercial assets fall under their purview for the defense of space. Formal arrangements that commit commercial assets as integral to military resiliency, for example the commercial *MAXAR* imaging satellites, might make them more likely to be targeted in times of conflict, so they, too, will need protection.[36]

Ultimately, the best defense is to have robust deterrents. Adversaries can be deterred from space engagements if they believe that their space operations can be countered, either by rendering attacks ineffective, or by exposing vulnerability to an in-kind response that destroys their capabilities (or even incurs some detrimental action in an unrelated regime). "Tit-for-tat" responses should assiduously avoid creating debris fields in space. Responses do not necessarily have to occur in space, but likely are most effective as deterrents if they can be demonstrated in space.

It is a much larger topic, but deterrence goes beyond simply deterring malevolent behavior. Counterspace capabilities are needed to deter adversary satellites from participating in military operations during combat. This can be done in space or ground operations, using a variety of the methods previously described as threats. More than just fielding one (or a few) of these techniques, the US should develop all such capabilities and more. This provides greater flexibility in conflicts and allows the nation to better develop and test effective defenses.

DOCTRINE, ORGANIZATION, AND POLICY

In 2023, the Department of Defense reviewed its space policies, and reported to Congress in response to congressional actions of the FY23 National Defense Authorization Act.[37] The report reiterated the strategy to defend US space capabilities and to deter hostile actions.

As part of achieving *Competitive Endurance*, the US Space Force has asserted the following tenets: the US should 1) avoid operational surprise, 2) deny first-mover advantages in space, and 3) be able to conduct responsible counter-space operations.[38] The implication is that the US should have precise intelligence concerning the orbits and functions of adversary satellites to render adversarial attacks ineffective, and should possess the ability to inflict damage to adversaries' satellites in both offensive and defensive operations.

Being aware of satellites in space is difficult; knowing their true purpose and their functionality is especially difficult. Preventing a surprise attack may require countermeasures that can be applied in advance of an attack. Deterrence may further require that assets be made defendable. "Responsible counterspace" requires policy decisions that permit the fielding of both defensive and offensive space assets.

There is a hope that acquiring the right kind of assets (i.e., both defense systems and counter space weapons), together with training of Guardians, will address these challenges. But this strategy may lead to point solutions that are easily countered with counter-counter capabilities. In this light, an agile and responsive acquisition strategy will not be enough.

For example, the US Space Force needs to develop doctrine for responses to threats. Suppose an unknown satellite approaches within a few meters of a US reconnaissance satellite worth billions of dollars. Should the US "take out" the approaching satellite because it is too close (which might be viewed as an act of war) using any of the attack vectors discussed above? Is a satellite "too close" if it is in an orbit that makes it possible for it to reach a valuable asset within a half hour? Would statutory authority be required due to the War Powers Consultation Act?[39] Does such policy require a presidential decision? Lest these be considered hypothetical issues, consider that the Russian Cosmos 2576 satellite, launched May 16, 2024, was reportedly placed into an orbit from which it could easily reach the orbit of a high-value US reconnaissance satellite.[40]

Prior to any hostilities, the Space Force needs to establish deterrents. Ideally, deterrents would not reveal all of the attack capabilities that the US could employ. Logically, the Space Force would demonstrate certain capabilities, but keep others in reserve for wartime contingencies. Might this deter the use of would-be attack satellites pre-positioned for offensive operations?

An integrated defense strategy is needed. When confronted with threats from the Soviet Union's nuclear weapons capabilities, the US created multiple commissions, enlisted leading scientists and strategists, established Federal Research and Development agencies (now DoD Federally Funded Research and Development Centers [FFRDCs]), and created a defense industrial base.[41] The integrated defense strategy is an inherent government responsibility, which requires the best minds and employs the most capable industrial partners.

These considerations are at a level above the Space Force, as currently organized, since the Space Force mission is fielding, equipping, training, and operating a military service.[42] Strategic integration decisions are at the level of the Assistant Secretary of the Air Force for Space Acquisition and Integration (who is also the Space Acquisition Executive), reporting to the Secretary of the Department of the Air Force and to the National Security offices of the Administration. However, the office of the Assistant Secretary must do more than architect the space assets needed across the government to ensure that defense systems are integrated. The architecture must depend on a strategy that solves the wicked problems of a contested space environment, and how to transition from the current state of an assumed uncontested environment.

This is not to suggest that the US Space Force is unaware of the issues or that the nation is not developing an effective strategy for contested space. Much of that strategy will necessarily be kept secret. Indeed, there is an existing DoD space strategy, a National Security Space Strategy, and a Space Force Commercial Integration Space Strategy.[43] These are high-level strategies that establish a demand signal to defense and commercial industries. They assert that there will be collaboration with industry, allies, and partners to produce solutions for space capabilities. Further, Aerospace Corporation serves as the principle FFRDC to the Space Force,[44] and in turn, involves companies, academics, and experts. There are Defense Science Board studies related to space capabilities and commercial space integration.[45] Other DoD advisory boards have also addressed threats and capabilities for space defense.[46]

NEED FOR INTEGRATED TECHNICAL SOLUTIONS

To muster the best minds, engage industry (both defense industries and commercial industries), and establish effective deterrents, at least some portion of a detailed technical strategy and desired capabilities need to be communicated and made apparent to appropriate stakeholders. Technical aspirations need to be articulated in a manner that is apolitical, with the full consent of the defense and intelligence committees, appropriators, and relevant military and civilian space communities. Capabilities need to be demonstrated to establish effective deterrents.

Technical developments are taking place; however, there are distributed voices and limited communication, and the commercial industry, in particular, has questioned how *Competitive Endurance* can be achieved. Time is short, and many believe that the US is playing catch-up in certain areas of space technology. As with other wicked national security challenges, the United States will need superb integrated technical solutions.

While an overall solution certainly presents a wicked challenge, there are certain directions that should be pursued toward a more integrated space defense posture.

First, since ground systems are an easy target for adversaries, resources need to be focused on defending and securing the ground receivers and stations. Initiatives can include better cyberdefense, more secure communications to space, freedom from local jamming attacks, more secure communications among ground nodes, and greater system redundancy. Money and effort spent on securing ground assets will force adversaries to consider far more costly strategies involving assets in space.

To defend US assets in space, a two-pronged approach will depend on the kind of assets that must be defended. In the past, operators of national reconnaissance and surveillance assets operating in space recognized that spacecraft were increasingly vulnerable to adversaries, many of whom were developing new space capabilities. At present, our most valuable space assets (including the several dozen GPS satellites and certain very valuable reconnaissance and surveillance satellites) require defense. A viable counterspace capability, fortified by doctrine, can help provide deterrence, but the US should consider battle spacecraft that can accompany and defend the most valuable space assets.

However, as noted, the main defense approach will likely involve proliferated satellite constellations. Such distributed architectures provide greater defense (resilience) and offer opportunities for more persistent coverage at lower altitudes. The US should not rely solely on commercial distributed assets (along with the Space Development Agency's tranches of satellites). Instead, many of the national capabilities that currently rely on small numbers of high-value assets need to migrate to proliferated architectures of small satellites, which might be attritable, without fully compromising their missions.

A major engineering challenge is to achieve equivalent technical capabilities using multiple small satellites with much smaller payloads that might individually be less capable. Solutions will require perceptive threat modeling leading to inciteful designs for mission payloads in families of space assets. Synergism among the downsized payloads will be needed to achieve the required mission performance. For example, super-resolution techniques based on multiple looks can be developed using distributed optical sensors.

SUMMARY AND RECOMMENDATIONS

The US military and many civilian systems are dependent on space assets. Over time, these space assets have become vulnerable to attack as space has evolved from uncontested to a contested battlespace. The US Space Force is charged with defending our national assets and capabilities in space. This wicked problem is not easily solved by simply procuring a few new systems. We have compared this challenge to those transformational challenges in the past that required multiple, integrated systems, as well as new doctrines and policy.

Our recommendations point in directions to mitigate risks. We recommend prioritizing the defense of ground stations due to their high vulnerability. We also emphasize that both our historical and new high-value large space assets can be protected through deterrence and defense adjunctive assets, and that the future of most space missions will be in proliferated architectures, which must be designed in ways that can maintain technical capabilities against a range of current and likely future threats.

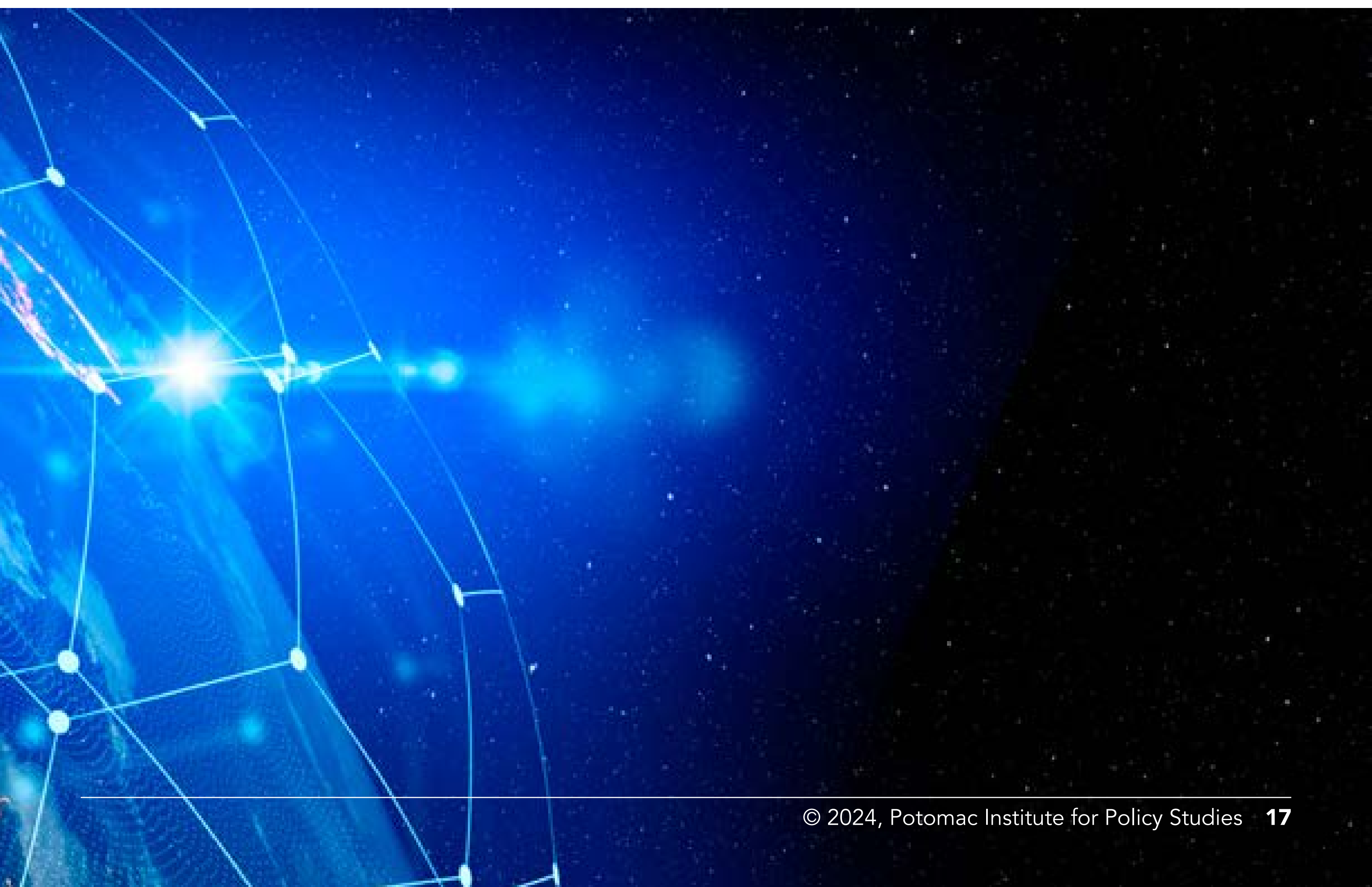
The US Space Force must thoroughly explore the issues underlying this transformation to a contested space environment. This task is complicated by the involvement of other bodies with whom the US Space Force shares authority, responsibility, and capability in executing US national security space missions. All of these entities must participate in a comprehensive study to ensure coordinated paths forward. These paths must address threats, vulnerabilities, evolving doctrines and policies, and potential technical solutions that contribute to a dominant space architecture.

Such a study will develop many specific conclusions and recommendations. Based on our summary considerations explored in this article, we offer the following likely determinations:

- Focus first on the defense of ground stations, due to their high vulnerability;
- Recognize that our high-value large space assets must be protected through deterrence and defense adjunctive assets, at least in the near term; and
- Continue implementing proliferated architectures of smaller space segments, ensuring they are designed to maintain technical capabilities even as they become smaller and more cost-effective.

ACKNOWLEDGEMENTS

The authors wish to thank J.P. Parker for thoughtful comments, and Sharon Layani whose work at the Potomac Institute in support of Space Systems Command was the impetus for this work.



ENDNOTES

1 White Paper on Competitive Endurance, Office of the Chief of Space Operations, U.S. Space Force, https://www.spaceforce.mil/Portals/2/Documents/White_Paper_Summary_of_Competitive_Endurance.pdf.

2 David Vergun, Space Challenges Prompt DOD Response, Space Superiority, U.S. Department of Defense, 21 Aug. 2020, https://www.defense.gov/News/News-Stories/Article/Article/2321670/space-challenges-prompt-dod-response-space-superiority/.

3 *Problems of Air Defense: Final Report of Project Charles, Vol. I., Massachusetts Institute of Technology,* 01 Aug. 1951.

4 Globe Composite, A Brief History of Anti-Submarine Warfare, Globe Composite Solutions LLC, 2024, https://www.globecomposite.com/blog/history-anti-submarine-warfare.

5 9/11 Five Years Later: Successes and Challenges, U.S. Department of State, 20 Jan. 2009, https://georgewbush-whitehouse.archives.gov/nsc/waronterror/2006/.

6 Ben Dryer, Explainer: how hostile is space?, The Conversation, 06 Aug. 2014, Explainer: how hostile is space? https://theconversation.com/explainer-how-hostile-is-space-27903.

7 Joel Dillion, The Cat-and-Mouse Game, Booz Allen Hamilton, https://www.boozallen.com/insights/defense/the-cat-and-mouse-game.html .

8 U.S. Space Command Public Affairs Office, Russia conducts space-based anti-satellite weapons test, U.S. Space Command, 23 Jul. 2020, https://www.spacecom.mil/Newsroom/News/Article-Display/Article/2285098/russia-conducts-space-based-anti-satellite-weapons-test/.

9 Melissa Davey, 'We've left junk everwhere': why space pollution could be humanity's next big problem, The Guardian, 25 March 2017, https://www.theguardian.com/science/2017/mar/26/weve-left-junk-everywhere-why-space-pollution-could-be-humanitys-next-big-problem.

10 Lars Rose, "Review and assessment of select US space security technology proposals", Space Policy, Volume 24(4), Nov. 2008, Pages 208-213, https://www.sciencedirect.com/science/article/abs/pii/S0265964608000672?via%3Dihub.

11 Ken Moriyasu, China can 'grapple' US satellites with robotic arm, commander says, Nikkei Asia, 21 Apr. 2021, https://asia.nikkei.com/Politics/International-relations/US-China-tensions/China-can-grapple-US-satellites-with-robotic-arm-commander-says.

12 This happens in a fictional depiction in the James Bond movie from 1967, "You only live twice".

13 Sandra Erwin, Space domain awareness: A secret weapon against shadowy threats in orbit, Space News, 14 Apr. 2022, https://spacenews.com/space-domain-awareness-a-secret-weapon-against-shadowy-threats-in-orbit/.

14 Brian G. Chow and Henry Sokolski, U.S. satellites increasingly vulnerable to China's ground-based lasers, Space News, 10 Jul 2020, https://spacenews.com/op-ed-u-s-satellites-increasingly-vulnerable-to-chinas-ground-based-lasers/.

15 Brett Tingley, These 3 teams just hacked a US Air Force satellite in space… and won big cash prizes, Space.com, 16 Aug. 2023, https://www.space.com/satellite-hacking-hack-a-sat-competition-winners.

16 Pavel Velkovsky, Janani Mohan, and Maxwell Simon, Satellite Jamming, On The Radar, 03 Apr. 2019, https://ontheradar.csis.org/issue-briefs/satellite-jamming.

17 Space Segment, GPS.GOV, 28 June, 2022, https://www.gps.gov/systems/gps/space/.

18 Brad Plumer, Have we become too reliant on GPS? This satellite expert thinks so, Vox, 10 Apr. 2016, https://www.vox.com/2016/4/10/11379698/gps-navigation-brain-problems.

19 Selam Gebrekidan, et al., Why GPS is Under Attack, New York Times, 02 Jul. 2024, Why GPS Is Under Attack - The New York Times https://www.nytimes.com/interactive/2024/07/02/world/gps-threats.html.

20 Jon Skillings, "GPS at risk: Those signals are more vulnerable than you realize," CNET, 9 July 2001, https://www.cnet.com/science/gps-at-risk-those-signals-are-more-vulnerable-than-you-realize/.

21 Theresa Hutchins, "Ground system for jam- resistant GPS delayed again to July 2025 at earliest, Pentagon tester says," Breaking Defense, 2 Feb 2024, https://breakingdefense.com/2024/02/ground-system-for-jam-resistant-gps-delayed-again-to-july-2025-at-earliest-pentagon-tester-says/.

22 Defense Primer: Hypersonic Boost-Glide Weapons, Congressional Research Service, 30 Jan. 2024, https://crsreports.congress.gov/product/pdf/IF/IF11459/9.

23 Hypersonic Missile Defense: Issues for Congress, Congressional Research Service, 24 June 2024, https://crsreports.congress.gov/product/pdf/IF/IF11623/13.

24 Kelley M. Sayler, Hypersonic Weapons: Background and Issues for Congress (R45811), Congressional Research Service, 09 Feb. 2024, https://crsreports.congress.gov/product/details?prodcode=R45811.

25 Jeffery Lewis, China's Orbital Bombardment System is Big, Bad News – but Not a Breakthrough, Carnegie Endowment for International Peace, 19 Oct. 2021, https://carnegieendowment.org/programs/nuclear-policy/proliferation-news/chinas-orbital-bombardment-system-is-big-bad-newsbut-not-a-breakthrough.

26 https://nuke.fas.org/control/salt2/text/salt2-2.htm

27 Dmitry Filipoff, Fighting DMO, Pt. 8: China's Anti-ship Firepower and Mass Firing Schemes, Center for International Maritime Security, 01 May 2023, https://cimsec.org/fighting-dmo-pt-8-chinas-anti-ship-firepower-and-mass-firing-schemes/.

28 Sharon Weinberger, Hypersonic Missiles Are Game Changers, and America Doesn't Have Them, The Wall Street Journal, 18 Sept. 2023, https://www.wsj.com/politics/national-security/hypersonic-missiles-america-military-behind-936a3128.

29 The New Generation of Positioning, Navigation and Timing, Lockheed Martin Corporation, 2024, https://www.lockheedmartin.com/en-us/products/gps.html.

30 Jason Sherman, Hypersonic Weapons Can't Hide from New Eyes in Space, Scientific American, 18 Jan. 2022, https://www.scientificamerican.com/article/hypersonic-weapons-cant-hide-from-new-eyes-in-space/.

31 CSIS Missile Defense Project, Ground-based Interceptor (GBI), Missile Threat, 26 Jul. 2021, https://missilethreat.csis.org/defsys/gbi/.

32 Nathan Strout, "One military space agency's plan for 1,000 new satellites by 2026," C4ISRNet, 21 Jan 2020, https://www.c4isrnet.com/battlefield-tech/space/2020/01/21/one-military-space-agencys-plan-for-1000-new-satellites-by-2026/.

33 Dave Schafer, Project Kuiper vs. Starlink, Satellite Internet, 19 Jan. 2024, https://www.satelliteinternet.com/resources/project-kuiper-vs-starlink/.

34 Planet website: https://www.planet.com.

35 HawkEye 360 website: https://www.he360.com.

36 Brett Tingley, Russia says private satellites could become 'legitimate target' during wartime, Space.com, 16 Sept. 2022, https://www.space.com/russia-private-satellites-legitimate-target-wartime-united-nations.

37 Space Policy Review and Strategy on Protection of Satellites, U.S. Department of Defense, 12 Sept. 2023, https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/COMPREHENSIVE-REPORT-FOR-RELEASE.PDF.

38 White Paper on Competitive Endurance, Office of the Chief of Space Operations, U.S. Space Force, https://www.spaceforce.mil/Portals/2/Documents/White_Paper_Summary_of_Competitive_Endurance.pdf.

39 S. 1939 – 113th Congress (2013-2014): War Powers Consultation Act of 2014, 16 Jan. 2014, https://www.congress.gov/bill/113th-congress/senate-bill/1939.

40 Jeff Foust, "US claims recently launched Russian satellite is an ASAT," SPACENEWS, 21 May 2024, https://spacenews.com/u-s-claims-recently-launched-russian-satellite-is-an-asat/.

41 Zachary J. Lemnios, US National Security in a New Era of Intense Global Competition, STEPS, 05 Apr. 2022, https://www.potomacinstitute.org/steps/index.php/issues/april-2022/us-national-security-in-a-new-era-of-intense-global-competition.

42 Space Force Public Affairs, Space Force begins transition into field organizational structure, U.S. Space Force, 24 Jul. 2020, https://www.spaceforce.mil/News/Article/2287005/space-force-begins-transition-into-field-organizational-structure/.

43 U.S. Space Force Commercial Space Strategy, U.S. Space Force, 08 Apr. 2024, https://www.spaceforce.mil/Portals/2/Documents/Space%20Policy/USSF_Commercial_Space_Strategy.pdf.

44 Dedicated to the Space Enterprise, Aerospace, 2024, https://aerospace.org/dedicated-space-enterprise.

45 Defense Science Board (DSB) Website: https://dsb.cto.mil .

46 For example, the Department of the Air Force Science Advisory Board, https://www.scientificadvisoryboard.af.mil/.

Technology Opportunities for National Prosperity

Rosalie Loewen

Research Economist,
Potomac Institute for Policy Studies

and

Robert Hummel

Chief Scientist,
Potomac Institute for Policy Studies

INTRODUCTION

Advances in science and technology present key moments for economic growth. Technological breakthroughs represent opportunities to make targeted public investments and introduce policies that accelerate time to market and incentivize market uptake, maximizing benefits for the domestic economy. The nation should capitalize on these opportunities through strategic investments and policies.

This is "industrial policy." Industrial policy can be defined as "targeted government interventions aimed at supporting specific firms, industries, or other narrowly defined economic activities to achieve national objectives."[1]

This paper identifies three technology areas with potential for significant returns if supported by appropriate US industrial policy. These areas were chosen based on criteria for when public interventions are more likely to have beneficial outcomes in a market economy for new technologies.

In a perfect economic world, industrial policy might never be required because it leads to inefficiencies in production in both theory and practice. However, in our real-world context—characterized by inefficient and distorted markets, unsatisfactory distributions of benefits, geopolitical tensions, and competition between national adversaries—the question is not whether to engage in industrial policy, but rather how to do it wisely.

The challenges associated with using industrial policy include: Determining when to use industrial policy (i.e., when the benefits are likely to outweigh costs), and understanding the distribution of those costs and benefits; and understanding which policies and interventions are likely to have better outcomes compared to other possible policies and interventions.

Technology innovation creates an environment in which industrial policy becomes more compelling. Industrial policy can accelerate the adoption of innovative products to increase total benefits. For example, public investment in a faster vaccine development cycle, despite its higher costs, can save more lives. Technological advances can provide high first-to-market payoffs and can create winner-take-all markets for which nations can compete. [2] National security applications might also require government intervention to ensure control over new technology.[3] Whether for national security or economic benefit, industrial policy is particularly tempting in an adversarial global environment when nations are willing to pay a price to ensure relative advantage over rivals.

WHEN IS INDUSTRIAL POLICY APPROPRIATE FOR R&D

Industrial policy engenders healthy debate in part because the government is using public resources to privilege certain sectors.[4] All industries can benefit from good policies such as having infrastructure or standards that create common solutions to shared problems. However, beyond supporting good policies broadly, government promotion of research and development will often choose certain areas of innovation over others. If the research applies to a large set of possible economic sectors, one can argue that the selection does not constitute industrial policy. In other cases, the potential application domain will be a narrow set of economic sectors, in which case the selection qualifies as industrial policy. The question then becomes:

What areas of innovation should the government select for industrial policy attention?

Policymakers should use the overlapping criteria for selection that are displayed in the accompanying box on page 23.

Focus on areas where innovation has a potential for big structural-level changes.

In some cases, innovation doesn't just improve a system or product but changes the whole system. If the change is substantial and positive enough, policies that accelerate production and bring society more quickly onto a new and better course can yield an outsized payout. Sometimes the right intervention is to remove obstacles rather than to build protection.

Consider where innovation may create first-to-market benefits and/or winner-take-all dominance in competition with adversaries.

Market intervention may outweigh the costs when innovation aligns with first-to-market benefits. In some cases, the first to market sets the standards for the international community or captures the market and dominates production, independent of who had the idea first.

Consider whether national security ramifications might be serious enough to weight the scales of a market cost-benefit analyses.

Research seeking to secure a national security advantage often justifies industrial policy. However, this can be a slippery slope in that any area can be presented as a question of national security.[5] Certain items, such as weapons and missiles, are clearly of national security importance. Other items, such as drones or satellite communications, might have sufficient market pull outside the defense establishment that government interest should be measured according to the relative national security importance.

Examine whether the technical innovation offers an opportunity to correct a market failure.

One form of market failure involves the tragedy of the commons, when broad harm can occur due to the distribution of a product without a clear payer to remediate (or pay for) the harm.[6] Conversely, market failure can occur when a product with broad benefits lacks a clear path to profitability.[7] Certain health products with limited markets exhibit this failure.

Corrections for market failures can lead to a more optimal outcome. For example, when technical innovation creates a more sustainable substitute for a natural resource that must be extracted using mining, it may be difficult to bring the substitute to market because natural resource extractors do not pay the cost of the environmental damage. The same argument could be made for products that reduce pollution when the polluters do not bear the full burden of their actions.

The following sections discuss sample application areas that might justify industrial policy actions based on one or more of these criteria. For each area, we describe the concept, discuss its importance, highlight current government and business activities, and suggest why further government intervention might be warranted. For each, we also provide some hints as to the kinds of technology developments and interventions that might support the applications for that area.

BIOTECHNOLOGIES FOR DIVERSE APPLICATIONS

The world has learned how to manipulate biology for human purposes. The development of these technologies has been a process of discovery and experimentation spanning centuries, accelerating to a crescendo with the recent breakthrough advancements in gene editing. The rapid development of a new type of vaccine to combat the COVID-19 virus is the most visible application of this new technology. However, many other applications are envisioned in fields as diverse as healthcare, materials science, textiles, energy production and storage, pollution remediation, data storage.[8] Biotechnology holds the potential for great societal benefits, but also carries the potential for harm.

The emerging beneficial biotechnologies will have a profound impact. Similar to the impact of microelectronics in the twentieth century, we can expect biotechnology to produce applications that people use and rely upon daily. Some of these innovations will harness natural biological systems to produce useful products, while others will employ synthetic biology to create new biological forms used for production. Applications will include sensors and therapeutics for healthcare, for example to both detect and treat diseases. However, significant applications extend beyond healthcare to include agriculture and food production, environmental sensing and remediation, energy production and storage, and manufacturing with new biologically produced materials.

Recognizing the advances in biotechnology and its importance to future economic and defense applications, the US government has used industrial policy in many ways to advance biotechnology (see box, below). These efforts, and others, are industrial policy because they support a specific sector, and in the case of Operation Warp Speed, specific selected companies.

- NIH's National Human Genome Research Institute advancement of genomics through The Human Genome Project (Oct 1990 to Apr 2003)
- The founding of a Biomedical Advanced Research and Development Authority within the Department of HHS (2006)
- Initiation of a Biotechnologies Office (BTO) at DARPA, 2014.
- The National Center for Biotechnology Information as part of the National Library of Medicine at NIH.
- Operation Warp Speed, a public-private partnership to accelerate the development and manufacture of vaccines to counter COVID-19; begun May 2020
- Executive Order on Advancing Biotechnology and Biomanufacturing Innovation for a Sustainable, Safe, and Secure American Bioeconomy, (Sept 2022)
- The National Biotechnology and Biomanufacturing Initiative, with investments and resources announced at a summit (Sept 2022)
- Establishment of the Advanced Research Projects Agency for Health, 2022
- DoD's release of a Biomanufacturing Strategy (Mar 2023)
- Congress's creation of a National Security Commission on Emerging Biotechnology (2023-24)

The marketplace is also a driving force behind biotechnology activities. According to the Biotechnologies Innovation Organization (BIO, an industry association), venture capital investments have amounted to tens of billions of dollars annually for the past half-decade to promote biotechnology research in anticipation of a burgeoning market for products.[9] While the 2021 pandemic expanded interest in biotechnology, it largely focused investments on health-related applications.

Given the availability of government and non-government funding, the appropriateness of industrial policy for biotechnology R&D lies in its relation to national security issues as well as a drive to accelerate developments across multiple application domains.

For example, while healthcare applications are important and lucrative for investors, they should not exclude development of other application areas, such as new applications for materials, agriculture, and energy production and storage.[10] Because these other applications may involve greater risk or require more time to scale to production, they risk being crowded out. Where investors are impatient, the government is often a successful and patient investor in early-stage research that pays off for the nation over time. Examples of this patient early investor approach include the National Institutes of Health (NIH) and the Defense Advanced Research Projects Agency (DARPA).

Even within healthcare applications, the development of vaccines, diagnostics, and one-time therapeutics should be pursued with equal vigor as the development of more lucrative maintenance drugs.[11] Market forces discourage investment in curative drugs and solutions for rare conditions. Yet, one-time vaccines and cures can be equally important for societal benefits.

Government support of infrastructure, including education, is a good candidate for positive intervention. The research environment and infrastructure supporting biotechnology should be maintained to attract the best minds and talent both domestically and internationally. Maintaining state-of-the-art infrastructure is a continuous pursuit. In some cases, shared laboratories and facilities can increase efficiency and safety, shared or incentivized by government sponsorship.

The talents and resources of academia as well as the private investment community need to be leveraged for national benefit. The biotechnology area offers numerous opportunities for "dual-use" applications, and public-private partnerships can accelerate the transition of technologies to address national needs. Government's role in these partnerships can make high-risk development areas more attractive.

Government intervention in the marketplace of ideas in biotechnology is justified to the extent that it encourages a balance of different directions. By being an early investor in the overlooked applications of biotechnology, including basic research, we can maximize the benefit and the likelihood of leading across multiple sectors.

CREATING COMMUNITIES USING VIRTUAL PRESENCE

The COVID-19 pandemic accelerated our understanding of remote collaborative work, both in government and business. Virtual presence also began to infiltrate civic communities.

However, the use of online virtual presence software barely scratches the surface of what is possible with broadband access and digital technology. Currently, remote virtual presence is a poor substitute for physical presence, even though remote working has transformed corporate work practices.[12] The innovation portion of productivity is diminished by the current forms of remote work and remote presence, and better applications are needed.

Concepts for a superior convergence of virtual and physical presence envision future environments as a "metaverse" with immersive technologies such as virtual reality, augmented reality, and mixed reality.[13] Digital presence, augmented with robotics, has the potential to revolutionize communications, education, business, healthcare services, design and manufacturing, senior care, and entertainment. Corporate work environments and innovation could also benefit from better virtual presence. However, while we can foresee a massive transformation, these technologies have yet to impact workflows.

Government-funded research has pursued augmented reality and virtual reality (AR/VR) over many years. Industry attempts to transition technologies using head-mounted displays, such as the Oculus Rift,[14] have had limited success. Other academic research led to the CAVE® system, now marketed by Visbox, providing embedded virtual reality,[15] which is used for training and product design.

Admittedly, the metaverse has been much hyped and thus much maligned. It is associated with computer games and bulky virtual reality headsets, as well as social media interactions that can be especially harmful to youth. But the real opportunity lies in empowering communities to thrive with the efficiency of digital communications, enabling individuals to interact intellectually and visually to exchange ideas, emotions, experiences, and services.

The technology is moving forward slowly, hampered by the need for capital investments and a societal impact application domain.

The objective concept requires more hardware than a desktop and flatscreen monitor and includes LED "walls" and rooms, eye trackers, 3D content generators, robots, 3D printers, and haptic devices.[16] The "metaverse" has not emerged in the way that is afforded by technology and that demonstrates its revolutionary potential for communities and society. Current approaches are still niche technologies with far greater potential. Greater investment in the supporting infrastructure might enable a flourishing of the capabilities to create communities.

While the commercial marketplace focuses on game technology, society should advance and leverage technology to benefit communities by creating greater efficiency in delivery of services. Market forces might find other applications that warrant investment, but the area of elder healthcare and wellbeing might justify industrial policy and serve as a prototype for other domains.

As demographic patterns force change, we can imagine and prepare for society's future needs. Virtual presence technologies for seniors can offer advanced services where the need is greater than other age groups and for whom the number of service providers is decreasing.[17] At the same time, technologies might enable seniors to be more productive for longer periods of their lives. Greater efficiencies and productivity levels in the older cohort can greatly benefit the total US economy.

Current approaches to assisted living and nursing care are unsustainable due to a dearth of available care workers. The percentage of people over 65 years old in the US has increased from 13.0% in 2010 to 16.8% in the 2020 census[18] and is expected to reach 20% in 2030.[19] To address this shift with fewer available caregivers, elder care needs to become far more efficient so that skilled caregivers can serve multiple patients.

Whether in residence or in their own homes, the use of virtual presence and robotic systems can help meet this need but requires investment in the development and emplacement of these systems. Equally important, virtual presence can allow at-home seniors and community residents to connect with family, friends, and others in distant locations with greater fidelity than current communications techniques allow. Senior living communities could co-invest in the infrastructure, to create better living environments and more efficient services.

Today, there is much effort in connecting all homes and businesses to high-speed internet service, which needs to be redoubled to utilize virtual presence technologies.[20] Low earth orbit satellite networks can be part of the process of connecting highly remote areas. However, the immersive technologies, robotics and haptics, and applications that provide services will require innovation and development, as offered by companies driven by market demand. Government can speed things along by encouraging infrastructure investments, driving to standards that bring interoperability, and representing the broader public and societal demand in arenas that may be less profitable.

INCREASING PRODUCTION CAPACITY USING ADVANCED DESIGN AND MANUFACTURING

The pandemic made clear the fragility of supply chains, affecting both defense systems and consumer goods. By beating out spare capacity in production, using just-in-time supply systems, and outsourcing large portions of our manufacturing capabilities, the US has become vulnerable to disruptions that are either inadvertent or deliberate, and so the US is challenged to provide surge capacity when needed. China has become a manufacturing powerhouse, and many US industries rely on Chinese manufacturing and assembly to provide production at scale.[21] As a result, certain design and manufacturing skills have atrophied in the US, as China has continued to hone its advanced manufacturing capabilities. The US has decided, for both national security and for greater economic independence, that the manufacturing capacity of the US needs to increase in many sectors.[22] Because the current labor environment of the US is limited, new approaches to manufacturing are required to succeed in increasing manufacturing capacity.

Today, factories use robotic pick-and-place machines and milling machines with computer numerical control (CNC) software to automate the manufacturing process of parts defined by computer-aided manufacturing (CAM) representations. While the underlying technologies have been in use for decades,[23] integrated facilities have not leveraged new technologies such as additive manufacturing, smart manufacturing, and mathematically sophisticated representation schemes. Modern technologies exist to make far more adaptable and automated manufacturing facilities that can utilize design assistants and digital designs to achieve scalable production of complex systems with mixed materials, which can be easily adapted or reprogrammed to manufacture other products, a concept known as smart manufacturing processes.[24] The US has invested in developing those technologies (see box). The challenge is to develop an industry of smart manufacturing, establishing a market for its services and products, and reducing the risks involved by creating partnerships of industries to choose advanced standards and interfaces.

Concepts for digital engineering and flexible automated manufacturing have been studied for many years and offer the opportunity for significant increases in efficiency and productivity. The US government fostered the National Network for Manufacturing Innovation (NNMI) program, which started in 2012 and established 17 public-private partnerships that operate under a *Manufacturing USA* umbrella to advance the future of US manufacturing through innovation, education, and collaboration.[25] The institutes vary from “America Makes” (researching 3D printing and additive manufacturing) to “BioMADE” (building a bioindustrial manufacturing ecosystem), and include the “Advanced Robotics for Manufacturing” (ARM) institute (developing new robotics and sensor technology for manufacturing) and CESMII, the Smart Manufacturing Institute (leveraging sensors and data in manufacturing for quality assurance and process improvement). The US Office of the Secretary of Defense (OSD) has a Defense Manufacturing Technology program (“ManTech”) to advance manufacturing technology for defense applications,[26] along with other initiatives for digital engineering. Legislation has been passed that requires systems engineering approaches with modular open systems and mission integration management for certain Department of Defense acquisitions.[27] The Boeing Corporation advertises their efforts in model-based engineering (MBE) for computational design in both their commercial and military programs, pioneering processes to accelerate an improved development and production of complex systems.[28] Air Force Research Labs has built “digital twins” of several existing weapon systems to perform virtual testing and analysis. Industrial design services, and educational programs at universities and learning centers to teach industrial design, includes a technology called “design for manufacturing and assembly” (DFMA) that emphasizes the process of designing parts for “manufacturability.” After up-front investments, digital engineering with advanced manufacturing capabilities can provide considerable savings in production and sustainment of products and, as a result, a market to support model-based engineering and digital design has been developing.[29]

And yet, China remains the world's leading manufacturer, with roughly three times the gross production (and twice the value-added) of US manufacturing, according to the Center for European Policy Research.[30] At one time, the differential was due to a lower cost of labor in China. While China continues to offer low-cost labor rates, there are alternative countries with lower rates, and China's labor costs have increased.[31] Advanced automated manufacturing should reduce needs for manual labor; the issue is capital investment in the capabilities to achieve the benefits across multiple application sectors. A detailed study published in *American Affairs* points to a widening gap between China's manufacturing capacity and US advanced manufacturing capabilities and bemoans the disconnect between the innovation ecosystem that designs products and the manufacturing capability to produce them.[32] They recommend specific actions to implement advanced manufacturing policies to promote new manufacturing technologies.

To date, the R&D efforts and industrial policy actions (which includes the CHIPS Act that subsidizes the construction of domestic semiconductor factories) have failed to revolutionize manufacturing and "move the needle" on US production capacity. Largely as a result, the US continues to run a balance of trade deficit with China, amounting to $280 billion in 2023.[33]

The market is challenged to induce the development of an advanced flexible manufacturing sector because the benefit would redound to a distributed set of companies and multinationals that currently forgo the profits from the manufacturing value add. There is an "activation" cost to implementing advanced manufacturing capabilities, and costs might initially be higher than those of outsourced manufacturing. The expertise in China, together with their reduced labor costs, provide a base that is hard to overcome. But a future of flexible automated manufacturing could potentially achieve lower-cost goods and more secure supplies compared to current operations.

The market also fails to value the benefits of controlling the manufacturing component of supply chains, instead assuming that external manufacturers would rarely cause disruptions in adversarial interaction. Proximity to production provides insights, process improvements, and innovation, which provide long-term societal benefits. For national security reasons, economic stability, and long-term benefits, advanced manufacturing needs to be reinvigorated in the US.

To bridge the gap from excellent R&D to implemented manufacturing facilities, and getting over the activation hump, government will need to corral multiple sectors and seed the development of pilot plants. How this should be accomplished, how much it costs, and who should pay will require study and ingenuity.

NEXT STEPS

We have highlighted three areas of opportunities in the science and technology domain:

- Biotechnologies for Diverse Applications;
- Creating Communities using Virtual Presence;
- Increasing Production Capacity using Advanced Design and Manufacturing; and

In each, we see how market forces have left opportunities unfilled, at least to date. It is possible that they might be filled given a little help. In many cases, that help might be considered industrial policy, and thus inefficient use of resources. But, with careful planning and analysis of the opportunities, policies might be crafted that bring new products and new capacities to fruition with minimal unwarranted intervention.

Admittedly, each area requires a more detailed technical analysis, and clear explanations to policymakers to justify interventionist actions. These areas were selected because we believe that such a case is supportable for each.

ACKNOWLEDGEMENTS

The ideas in this article have a genesis with too many to mention, but we specifically thank Al Shafer and Mike McGrath for insightful comments on certain technology opportunities.

ENDNOTES

1 International Monetary Fund, IMF e-Library, 11 March 2024, https://www.elibrary.imf.org/view/journals/007/2024/008/article-A001-en.xml.

2 Arnold, Roger A. (2007-01-25). *Economics*. Cengage Learning. ISBN 978-0324538014.

3 https://www.defense.gov/News/News-Stories/Article/Article/3644527/dod-releases-first-defense-industrial-strategy/.

4 Shantayanan Devarajan, "Three reasons why industrial policy fails," Brookings, Jan 14 2012, Three reasons why industrial policy fails, https://www.brookings.edu/articles/three-reasons-why-industrial-policy-fails/.

5 The White House, "Memorandum on Presidential Determination Pursuant to Section 303 of the Defense Production Act of 1950, as amended, on Insulation," Jun 6, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/06/06/memorandum-on-presidential-determination-pursuant-to-section-303-of-the-defense-production-act-of-1950-as-amended-on-insulation/.

6 Garrett Hardin, "Tragedy of the Commons," Econlib, https://www.econlib.org/library/Enc/TragedyoftheCommons.html.

7 Piirainen, K. A., et al., (2018). The reverse tragedy of the commons: an exploratory account of incentives for under-exploitation in an open innovation environment. *Technology Analysis and Strategic Management*, 30(3), 268-281. https://doi.org/10.1080/09537325.2017.1308479.

8 Timothy Bumpus, Sharon Layani, and Alyssa Adcock, "The Many Application Areas of Synthetic Biology," *STEPS* Issue 5 (2021), https://www.potomacinstitute.org/steps/index.php/issues/september-2021/synthetic-biology.

9 Bio (Biotechnology Innovation Organization), "The Venture Investor Outlook and Mindset," Apr 21, 2022, https://www.bio.org/webinars/raising-capital/venture-investor-outlook-mindset.

10 Jonathan Smith, "The biggest private biotech investments in Feb 2023,"LabioTech, Mar 2023, https://www.labiotech.eu/in-depth/biotech-investments-february-2023.

11 Bio, "New BIO Report finds more innovation and investment needed in vaccine development," Jan 25, 2024, https://www.bio.org/press-release/new-bio-report-finds-more-innovation-investment-needed-vaccine-development.

12 Danielle Abril, "Bosses say remote work kills culture. These companies disagree," *Washington Post*, Sept 1, 2022, https://www.washingtonpost.com/technology/2022/09/01/remote-work-culture/.

13 Janna Anderson and Lee Rainie, "The Metaverse in 2040," Pew Research Center, June 30, 2022, https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/.

14 Meta Quest, Oculus Rift website: https://www.oculus.com/rift-s/.

15 Visbox, "CAVE Automatic Visual Environment," website: http://www.visbox.com/products/cave/.

16 Yuxiang Shi and Guozhen Shen, "Haptic Sensing and Feedback Techniques toward Virtual Reality, PMC PubMed Central, NIH National Library of Medicine, Mar 23, 2024, doi: https://doi.org/10.34133%2Fresearch.0333.

17 The company Rendever® offers virtual reality headsets and immersive technology for seniors (Rendever | Virtual Reality for Seniors | VR for Healthier Communities).

18 Zoe Caplan, "U.S. Older Population Grew From 2010 to 2020 at Fastest Rate Since 1880 to 1890," US Gov't Census Bureau, May 2023, 2020 Census: 1 in 6 People in the United States Were 65 and Over.

19 Center for Elders and the Courts, a project of the National Council for State Courts, "Introduction, Demographics of the Aging Population," Introduction | Elders and Courts, https://www.eldersandcourts.org/aging/introduction.

20 USDA Department of Agriculture, "e-Connectivity for all rural Americans is a modern-day necessity," Broadband | USDA.

21 Richard Baldwin, "China is the world's sole manufacturing superpower: A line sketch of the rise," VoxEU, Center for Economic Policy Research (CEPR), Jan 17, 2024, https://cepr.org/voxeu/columns/china-worlds-sole-manufacturing-superpower-line-sketch-rise.

22 Devon Bistarskey, "U.S. Manufacturing Ecosystem Key to Economic Growth, Innovation, Competitiveness," U.S. Department of Defense defense.gov, Oct 14, 2022, https://www.defense.gov/News/News-Stories/Article/article/3189049/ .

23 TCM Toolcraft Machining, "CNC Machining: A Brief History of the Manufacturing Mainstay," Aug 19, 2022, https://www.toolcraft.com/blog/cnc-machining-a-brief-history/.

24 Yuqian Lu, Xun Xu, Lihui Wang, "Smart manufacturing process and system automation – A critical review of the standards and envisioned scenarios," Journal of Manufacturing Systems, Jul 2020, https://www.sciencedirect.com/science/article/abs/pii/S027861252030100X.

25 Manufacturing USA website: https://www.manufacturingusa.com.

26 https://www.dodmantech.mil/JDMTP/OSD-ManTech/.

27 Robert Gold, "System Integration Management," 20th NDIA SE Conference, https://ndiastorage.blob.core.usgovcloudapi.net/ndia/2017/systems/Wednesday/Track2/19849_Gold.pdf.

28 Boeing website, "Model-based engineering-What is it?", https://www.boeingsuppliers.com/modelbasedengineering.html.

29 Zuken Americas website, Shaping tomorrow: The unstoppable demand of digital engineering," https://www.zuken.com/us/blog/shaping-tomorrow-the-unstoppable-demand-of-digital-engineering/.

30 Richard Baldwin, voxEU, op. cit.

31 SCMR Staff, "China is no longer a low-cost labor country," Supply Chain Management Review, Oct 20,2022,https://www.scmr.com/article/china_is_no_longer_a_low_cost_labor_country.

32 David Adler and William B. Bonvillian, "America's Advanced Manufacturing Problem—and How to Fix It," *American Affairs Journal*, Fall 2023, https://americanaffairsjournal.org/2023/08/americas-advanced-manufacturing-problem-and-how-to-fix-it/.

33 Bureau of Economic Analysis, "US International Trade in Goods and Services, December and Annual 2023," Feb 2024, https://www.bea.gov/news/2024/us-international-trade-goods-and-services-december-and-annual-2023.

The Detrimental US Tax Policy on Research and Development

Robert Hummel

Chief Scientist, Potomac Institute for Policy Studies


TAX

US TAX POLICY ON R&D

The US Tax Code allows businesses and taxpayers to deduct what are called "research and experimentation expenses" from their income before paying taxes, provided those expenses are "qualified," according to Section 174 of the tax code. In addition, Section 41 permits a tax credit for increases in research and development (R&D) expenditures over a baseline amount, as long as those expenses qualify under Section 174 and satisfy certain other conditions. Section 174, as originally formulated, allowed a company to depreciate R&D expenses over five years, if the taxpayer so desired, enabling the deduction to apply when the fruits of R&D generated taxable returns. Seemingly, the US tax code treats R&D favorably.

However, this common perception is misleading; in reality, US tax policy is unfriendly to R&D funded by for-profit companies. The policy is complex, confusing, and counterproductive. Qualifying conditions make the tax code suspicious of companies claiming to conduct R&D. The tax code can be viewed as discouraging businesses from pursuing independent R&D that is not sponsored by the government or others. The provisions create a legal nightmare of subjective interpretations of R&D, and amount to a jobs program for lawyers and accountants in association with businesses' R&D operations. Both Sections 174 and Section 41 pose challenges.

Recent changes have made the situation much worse.

THE CHANGE TO R&D DEDUCTIBILITY

Starting in 2022, the US tax code changed how research and development (R&D) was treated with respect to taxes on earnings. Prior to 2022, taxpayers and businesses generally deducted "qualified" R&D expenses from their earnings before being taxed. The Tax Cuts and Jobs Act (TCJA) of 2017 mandated that R&D expenses be depreciated over a five-year period (fifteen years for foreign-based R&D) starting mid-2022, each and every year in which qualified R&D expenses were incurred. In converting from deducting expenses in the present year to amortizing deductions over five or more years, this provision constitutes a massive one-time tax increase. This change also diminishes the benefit of deducting R&D expenses for all future years, because a deduction today is more valuable than cumulative deductions spread over several years. The combined two effects constitute an attack on corporate R&D that has already resulted in reduced innovation and product development in the United States, and will continue to inhibit innovation.[1]

This change to the US tax code (replacing Section 174) in its treatment of R&D is so onerous that it was included as a provision of the TCJA with the likely intention that it should never be implemented.[2] Most taxpayers likely did not expect the provisions to survive.[3] It was added to reduce the 10-year cost of the TCJA by collecting extra taxes against companies conducting R&D, with an estimated revenue of over $100 billion for the Treasury within that timeframe.[4] Even beyond 2027, however, the requirement to depreciate R&D expenses will serve as a deterrent to R&D investments.

Congress is aware of the punitive nature of this change and its harmful consequences, but as of this writing, they have failed to rescind the provision.[5]

Taxing R&D is a misguided policy. Consider a for-profit company that conducts significant R&D. Like most such companies, they have been deducting those expenses from their earnings before taxes in the year incurred. However, in 2022, companies suddenly had to depreciate the expenses over five years, starting mid-year. Thus, in 2022, they could deduct only 10% of their R&D expenses, while the remaining 90% had to be taken from after-tax earnings, i.e., taken from their capital account. If they maintained the same level of R&D expenses in 2023, then in that year, they could deduct 20% of the 2022 expenses plus 10% of the new 2023 R&D expenses, leaving 70% of their R&D expenditures to come from the capital account. To pay the tax bill, they will likely reduce their R&D expenditures. However, if they maintain a level R&D commitment, they will have paid taxes on 250% of an annual R&D expenditure (of US R&D expenditures) over the five-year period starting mid-2022.[6] For such a company, this represents a massive tax burden. Even after 2027, any increases in R&D costs will come from capital accounts, and the present value of deductions will be less than current year expenditures, because future year depreciated deductions will be less valuable than current year deductions.

From the standpoint of businesses, they face paying a one-time tax over five-plus years on a substantial portion of current R&D. They will also pay a corporate income tax on some portion of their future ongoing R&D, due to the present value computation of a deferred deduction.

Taxing R&D contradicts what the nation should want. This is the era of advanced technology and geopolitical competition in technology development. The country with the best technology will win in military, economic, and political spheres. Technology advances are enabled by investment in R&D, and overall R&D investments have the greatest payoff among corporate investments. Congress has been seeking ways to boost the US innovation capacity,[7] to retain or attain leadership in science and technology fields and to translate those advances into market dominance. While the nation excels at research performed by universities and nonprofits, these results are often made public for the world to exploit. The nation needs a vital corporate research ecosystem to exploit technology advances to develop products for economic benefits.

But the US has been moving backwards in support for corporate R&D by virtue of tax policies.

WHY AREN'T RESEARCH EXPENDITURES DEDUCTIBLE?

The recent tax change to Section 174 constitutes a major policy issue. Likewise, the "R&D Tax Credit" of Section 41, which is actually a partial credit on incremental increases in R&D, is far too complex to be useful. But these sections of the tax code really highlight a more fundamental question: Why aren't R&D expenditures deductible as ordinary and necessary expenses?

Business expenses that are ordinary and necessary are deductible due to Section 162(a). When Section 174 was introduced in 1954, it may not have been clear that research and experimental expenditures were ordinary and necessary,

and so special provisions were included in Section 174(a) to settle the issue—Research expenditures related to the trade or business were deductible. Further, that section allowed those expenses to be depreciated over five or more years, permitting deductions to occur in years when the research might yield revenue. This provision was intended to make research that much more valuable, to reduce a business's after-tax expenditures on research.

Today, R&D expenses are not only ordinary expenditures for most companies but also necessary in the global competitive marketplace. R&D is the engine of US innovation and is critical to US future prosperity. Businesses, and especially high-technology businesses, need to conduct R&D to stay current and to keep ahead of the global competition. Without R&D, products stagnate and can be overtaken by alternatives in the march of technology. In some cases, companies must conduct R&D to reinvent themselves as legacy business lines become obsolete.

Businesses can deduct advertising and marketing costs, and most employee salaries are fully deductible. A business can deduct costs for lawyers and accountants who discern the qualified research and experimental expenditures.

It seems logical that companies should be allowed to deduct reasonable costs of R&D. Reimbursed expenditures are not deductible, and the issue is moot for nonprofits, such as public universities. But, for businesses that are for-profit, deductions should follow the usual rules for business expenses. Wages and benefits should be expensed in the year incurred, while equipment and supplies should be depreciated over reasonable schedules reflecting their useful lifetimes.

The mere existence of Section 174 suggests that certain R&D expenses are not deductible. The restrictions explicitly deny certain expenses as treatment under Section 174(a). Legal arguments might then attempt to argue that the same denied expenses could be treated as ordinary and necessary expenses under Section 162(a), but that argument is clearly a subterfuge that circumvents the intent of Section 174 and might not prevail in an audit. Moreover, Section 41 tax credits apply only to a portion of the expenditures that qualify under Section 174. If expenses were deducted using 162(a), they could no longer be counted toward Section 41.

When the corporate tax rate on profits was higher than typical marginal tax rates on wage income, restrictions were needed to prevent companies from performing distributions under the guise of research to hide profits. Thus, it made sense to circumscribe qualified research expenditures. However, the tax code became muddied in its attempts to define terms like "new information," "discovery," and "uncertainty." Most R&D is discernible based on the facts of the case. Reasonable expenditures depend on the kind of research being conducted and the level of wages necessary to obtain and retain the research talent. Distributions inappropriately labeled as "research," and unreasonable or excessive expenditures are likely easy to detect. Salaries for researchers will be taxed as income, potentially at a higher rate than current corporate tax rates.

THE DEPRECIATION MYTH OF R&D

The theory behind an amortization deduction is that an asset purchased in the taxable year has a useful lifespan and can be traded or sold for a decreasing value during its useful life. This clearly does not apply to R&D. While R&D can result in property (likely intellectual property [IP]), that IP should either be monetized quickly to reap benefits before competitors catch up, or the research may yield negative results, rendering the IP essentially worthless. However, even if the IP is valueless (the research did not pan out), the tax code insists that the deductions take place over at least five years. Speculative research that ends up going nowhere is still justifiable R&D. It is a myth that research always results in assets that remain useful to the business for the succeeding five years.

A sentence added to Section 174-2(a)(1) in 2014 emphasizes that the research or experimentation of Section 174 is expected to lead to a product: "The ultimate success, failure, sale, or use of the product is not relevant to a determination of eligibility under section 174."[8] This implies that Section 174 requires that intent of the research should be that it lead to a product, even if it is not accomplished. It does not seem to allow for the research that yields negative results before conceptualizing a product. It does not value exploratory research aimed at discovering new technologies when a specific product has not yet been determined.

A BOLD PROPOSAL

The US tax code needs to be rewritten regarding corporate R&D. Rather than further incremental changes that add to complexity and confusing provisions, we suggest that bold reforms are required. Details will need to be studied, and the analysis should consider the benefits of unleashing corporate R&D from bureaucratic overhead imposed by onerous tax accounting. We suggest that changes need to conform to the following:

- **Scrap Section 174 entirely.** Eliminate it. Amend Section 162 concerning ordinary and necessary business expenses to allow the deductibility of R&D expenses, expensed for wages and salaries of researchers subject to US income tax, and depreciated for assets that are used in research activities. Allow deductions for contracted services attributed to researchers and research activities. Section 162 should clarify that deductible expenses need to be reasonable according to market conditions. Allow for carry-forward of unused deductions to permit their application to revenue generated by the research.
- **Rewrite and rationalize Section 41.** Allow for investment tax credits for research in targeted research areas specified every five years by a government agency such as the National Science Board. Focus the credits on actual research activities by qualified researchers in the US compensated by businesses, and allow for carry-forward for the nonrefundable credits for up to five years to encourage application of the credits to revenue from products. Ensure that deductions apply only to that portion of research expenses not compensated by tax credits or external funding.
- **Simplify reporting requirements** so that research or experimentation expenses are deductible or eligible for credits based on simple, easily justified criteria. Set tax credit rates at percentages that incentivizes industry to perform legitimate research that strengthens US technology, without creating subsidiary businesses to help companies apply for credits. Focus credits on small and medium-sized businesses by emphasizing innovative and emerging technologies.

Due to institutional momentum ("we've always done it this way"), there will be considerable opposition to these common-sense reforms. There are vested interests in the complexity of the current code and a reluctance to encourage risk-taking in research endeavors. We need to get beyond these hesitations to retain a leadership position throughout all sectors of the innovation base, including our businesses that aim to profit. Whether the R&D is pursued in connection with a company's existing trade or business, or whether the R&D is pursued with the intention of reinventing a company's line of business, or creating a new line of business, the reasonable expenses for that research should be recognized as ordinary and necessary business expenses.

THE HISTORY OF HOW WE GOT HERE

In the tax code adopted in 1954, businesses in the US were allowed to deduct qualified research spending, either by "expensing" the deduction or amortizing the deduction according to a five-year depreciation schedule. The 1954 code, Section 174, specified that "research or experimental expenditures" (REEs) were considered deductible if they were "in connection with the trade or business." [9] The same tax law codified the deductibility of "ordinary and necessary expenses" in Section 162(a).

A business was allowed to choose the depreciation option, which allowed the taxpayer (the business) to ratably amortize REEs over five years, starting when the business begins to realize benefits from the research. The business was allowed to make this choice voluntarily, in which case all subsequent REEs would likewise be amortized over five years. In this case, the expenditures were called "specified research or experimental expenditures (SREs)." If a business is not yet profitable, deducting expenses over five years will result in deductions in later years, when the research is paying returns, making them more valuable than expensing the deduction in the year the expenses were incurred. So, some companies chose to depreciate R&D, while ongoing concerns with taxable revenue prefer expensing qualified R&D expenses as deductions in the year spent.[10] Neither option is as valuable as allowing carry-forward deductions, which was not authorized in the tax code.

In 1960, the definition of REEs were specified in Section 174-2 of the tax code with specific activities excluded from deductibility and, over time, illustrated with multiple examples.[11] REEs do not include quality control testing, efficiency surveys, management studies, consumer surveys, advertising or promotions, acquiring intellectual property, or historical research. Further, REEs include the notion that the research "would eliminate uncertainty concerning the development or improvement of a product."[12] Section 174-2(a)(9) dictates that REEs be "reasonable under the circumstances."

In 1981, Congress passed a temporary "Research and Development Tax Credit" that incentivized businesses to increase their investments of R&D.[13] The provision provided a partial credit (originally, 25%, and later 20%) for a limited increase in research expenditures over a base period. However, to incentivize particular kinds of research, eligible expenses were restricted to "qualified research expenses" (QREs) that excluded, for example, social science and humanities research and research conducted outside the United States. These provisions were extended and modified over the years, becoming known as Section 41,[14] and were made permanent in the tax code in 2015.[15] But in 1986, the research expenditures eligible for a partial credit, QREs, were further restricted,[16] explained as four tests to be conjunctively satisfied.[17] The legislative history of Section 41 includes numerous pauses and retroactive reinstatements, which limited the effectiveness.[18] In 2003, the "Discovery Rule" that required that qualified research had to be undertaken for the purpose of discovering information was loosened: Research that previously needed to be "new to the world" was changed to "new to the taxpayer."[19] In 2006, an "alternative simplified credit" was introduced, providing a somewhat simpler alternative to the complex task of computing the baseline research expenditures, but with more complex record-keeping requirements. Two other forms of credit have been added, including a partial credit for basic research and one for energy research, independent of the requirements for incremental increases.

The full complexity of Section 41 R&D tax credits is revealed in a Congressional Research Service analysis, last updated in July 2022,[20] which discusses various policy options to increase its effectiveness in spurring useful increases in domestic R&D. An appendix details the long and complex legislative history.[21] The upshot, however, is that Section 41 constitutes tax expenditures (lost tax revenue) for the US for the purpose of incentivizing corporate R&D in amounts exemplified by an analysis in the CRS report.[22] For example, in 2014, a Section 41 estimated tax expenditure of $12.6 billion, which supplemented $130 billion of federal R&D expenditures (grants and contracts) that added to business spending on domestic R&D of $341 billion (in that year). It is hard to know how much of that $341 billion was due to the existence of the Section 41 tax credits. As the CRS analysis makes clear, the computation of the credit is now ridiculously complicated, raising doubts about the effectiveness of Section 41.[23]

The change invoked by the Tax Cut and Jobs Act (TCJA) of 2017 (Public Law 115-97), Section 13206, put a spotlight on tax code sections 174 and 41, by substituting Section 174 with a new version. This act requires that REEs be depreciated over five years (and fifteen years for expenditures on research performed by foreign concerns) beginning in 2022, eliminating the expensing option. A significant burden fell on microelectronics firms,[24] which normally carry on a great deal of R&D in a race to be first to market with the latest semiconductors. However, software development companies, pharmaceuticals, and various other development sectors are accustomed to expensing research expenditures and have especially suffered from this change.

The US has a long tradition of R&D investment through direct grants, contracted research, and the procurement of items requiring development to meet specifications. The defense industrial base receives funding for independent research and development (IRAD). But globally, an increasing amount of R&D is conducted by independent for-profit companies. In China, companies receive direct subsidies for research in certain targeted areas, as prescribed by the "Made in China 2025" program.[25] In comparison, the US Section 41 incremental and partial tax credits are quite limited.

ACKNOWLEDGEMENTS

The author thanks Brian Shirley, member of the Board of Regents of the Potomac Institute, for helpful comments, and the staff of the Potomac Institute for their support.

ENDNOTES

1 Mary Coxx et. al., "The Consequences of Limiting the Tax Deductibility of R&D," Graduate School of Stanford Business, Working Paper 4192, Jul 2024, https://www.gsb.stanford.edu/faculty-research/working-papers/consequences-limiting-tax-deductibility-research-development.

2 Congressional Research Service, CRS INSIGHT, IN-11479, Aug 2020, https://crsreports.congress.gov/product/pdf/IN/IN11479.

3 Greg Sweigart, J.D. Denver, "Rights for the R&D Tax Credit and Sec. 174" in The Tax Advisor, Jun 2024, https://www.thetaxadviser.com/issues/2024/jun/rights-for-the-research-development-credit-and-sec-174.html.

4 Congressional Research Service, "Tax Treatment of Research Expenses, Current Law and Policy Issues," Dec 19,2022, https://crsreports.congress.gov/product/pdf/IN/IN11887.

5 ABGi, (A tax consulting firm), "Section 174: Latest News and Updates," https://abgi-usa.com/section174/latest-and-greatest.

6 For a constant level of foreign R&D expenditures, the computation leads to 750% of an annual R&D expenditure that will be subject to taxes over the fifteen year period.

7 See Section 889 of the "William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021," https://www.congress.gov/116/plaws/publ283/PLAW-116publ283.pdf.

8 26 CFR § 1.174-2 - Definition of research and experimental expenditures.

9 Internal Revenue Code of 1954, Chapter 1, Subchapter B, Part VI, Itemized Deductions for Individuals and Corporations, Section 174, pg 66, https://www.govinfo.gov/content/pkg/STATUTE-68/pdf/STATUTE-68A-Pg1.pdf.

10 However, since 2022, all REEs are considered SREs, and businesses are required to depreciate SREs over five years (and fifteen years for foreign research). Further, the depreciation schedule must begin in the year in which the expenses occur.

11 Published in the Federal Register, 1960, page 11573, https://www.govinfo.gov/content/pkg/FR-1960-11-26/pdf/FR-1960-11-26.pdf, Last version of 174-2 is found in https://www.law.cornell.edu/cfr/text/26/1.174-2.

12 Bloomberg Tax, "R&D Tax Credit and Deductions," Jan 26, 2024, https://pro.bloombergtax.com/insights/corporate-tax-planning/rd-tax-credit-and-deducting-rd-expenditures/.

13 Public Law 97-34, Aug 13, 1981, Section 221, https://www.congress.gov/97/statute/STATUTE-95/STATUTE-95-Pg172.pdf.

14 Taxnotes, "Section 41, Early Legislative History," https://www.taxnotes.com/research/federal/usc26/41/early-legislative-history.

15 Bloomberg Tax, "R&D Tax Credits and Deductions," Jan 2024, https://www.taxnotes.com/research/federal/usc26/41/early-legislative-history.

16 Gary Guenther, Congressional Research Service, "Federal Research Tax Credit: Current Law," Last Updated July 27, 2022, CRS Report RL31181, https://crsreports.congress.gov/product/pdf/RL/RL31181, see page 30.

17 Four tests remain in place, although changed. See https://warrenaverett.com/insights/what-are-qualified-activities-and-expenses-for-the-rd-tax-credit/.

18 Taxnotes op. cit.

19 https://www.alliantgroup.com/services/r-d-tax-credit-2/evolution-of-the-rd-tax-credit/.

20 Gary Guenther, op. cit.

21 Ibid, Appendix A.

22 Ibid, Table 3.

23 Ibid. Page 12.

24 Brian Shirley, "Want US Semiconductor Leadership? Fox the Tax Code," STEPS: Science Technology, Engineering and Policy Studies, Issue 8, pp 18-28, 2023, https://www.potomacinstitute.org/steps/images/PDF/TaxCodeSingle.pdf.

25 Institute for Security and Development Policy, "Made in China 2025," June 2018, https://www.isdp.eu/wp-content/uploads/2018/06/Made-in-China-Backgrounder.pdf.

Mitigating Algorithmic Targeting in Social Media Platforms

Kayla Dunn
Potomac Institute for Policy Studies Intern, Summer 2024, and Student, Georgetown University


You
Tube
You
Tube

It is now well understood that social media platforms collect data about their users. The platforms gather this data to push content that supports targeted advertisements. This business model incentivizes platforms to maximize user engagement and disseminate content that negatively impacts society. Notably, misinformation, disinformation, and mal-information demonstrably generate higher levels of engagement.

Platforms claim they collect user data to personalize and improve the user experience. For example, TikTok and Meta platforms utilize data to craft their "For You Page" and "Recommended Posts," respectively. However, this language obscures other motivations for user data collection, including targeted advertising. Today, no one doubts that these platforms collect user data, but the extent and purpose of this collection are often overlooked.

Social media platforms collect user data in four ways:

1. **User-provided data**: Data a user produces, including posts, searches, comments, "likes," content viewed, content engagement levels, and user profile information such as email addresses, phone numbers, and contacts.[1]
2. **Device information**: Data from the devices users use to access the social media platform, such as device model, software, location, photo access, and network connection information.
3. **Data collected from other users**: Posts by other users on the platform that tag or mention the user, networks of users including "friends" and who is "followed," and search histories that involve users.[2]
4. **Third-party data**: Data shared from external sources, such as other platforms and browsers, websites visited via social media platforms, cookies, and third-party location.[3]

Ad targeting begins when an advertising company contacts a social media company with an ad campaign. The advertising company has a specific demographic they want to target. The social media company then asks the advertising company about their budget for the advertising campaign. In essence, the advertising company bids for advertising space for their campaign, with a separate price for a liked post, an ad that is followed with a click, a website that is visited, and potentially even a sale that occurs as the result of the ad on the social media company's platform. The social media company can execute the auction as real-time bidding, or have predetermined prices in advance for targeted advertising. Either way, the social media company is now highly motivated to (1) have as many people as possible of the targeted demographic spend plenty of time on their platform, and (2) to present the ad to precisely targeted users to maximize what is called "click-through rate," i.e., the likelihood that the ad will generate revenue through a charge to the advertiser.

Advertising rates increase proportionally to users' engagement level on the platform. When the social media company optimizes its targeted demographics, clicks will be more likely and more frequent. To achieve high levels of engagement, social media companies benefit when a post or video goes "viral." Every interaction can refine algorithms targeting users. This transactional relationship places utmost importance on social media platforms increasing engagement levels through continuous manipulation and revision of platform targeting approaches. This process is meticulous. It encourages viral posts and sustained interactions.

Further, the quality of content is not the primary concern of social media companies; their main interest lies in the level of engagement with their content and the likelihood of ads generating revenue through "clicks." Research confirms that content achieving the highest levels of engagement is mis-, dis-, and mal-information. On Twitter (now known as X), studies have shown that "falsehoods were 70% more likely to be retweeted than the truth."[4] On TikTok, a 2022 study by NewsGuard found that "almost 20 percent of the videos presented as search results contained misinformation."[5] On Facebook, a study conducted by a joint research team at the University of Southern California found that "frequent, habitual users forwarded six times more fake news than occasional or new users."[6] This is a symptom of the social media business model; content that garners engagement is rewarded regardless of quality.

Social media companies and those selling ad space typically utilize proprietary AI algorithms that leverage collected data to profile and characterize each user. This has revolutionized the advertising business. "Data commercialization" includes the entire process of developing and presenting content, and collecting, characterizing, and placing targeted ads.

The effect of data commercialization is evident through the rapid growth of social media advertising revenue. In the two decades following the founding of Facebook in 2004, social media advertising has become a multi-billion-dollar industry. For example, Meta earned $38.7 billion[7] in advertising revenue in Q4 2023 and Tik Tok generated $14.5

billion[8] in advertising revenue in 2023. Another estimate suggests TikTok generated $16.1 billion in 2023, a 67% increase year-on-year.[9] Currently, global spending on social media advertising is approximately $270 billion,[10] with that figure forecasted to increase to $345.73 billion by 2029.[11] Advertising in the United States has consistently remained around 2% of GDP since the 1920s.[12] Social media companies and online platforms are taking an increasing share.

CURRENT LEGISLATION

Governments globally have recognized that data commercialization is a problem. One primary concern is the proliferation of misinformation, disinformation, and malinformation. Various social ills, some resulting from these issues, have been ascribed to data commercialization.

In response, governments have introduced certain regulations. Foundational regulations in this field include:

- Section 230 of the Telecommunications Decency Act of 1996;
- The General Data Protection Regulation of 2016 (GDPR);
- The California Consumer Privacy Act of 2018 (CCPA); and
- European Union's Digital Services Act of 2022 (DSA).

Other laws and regulatory measures are currently being debated throughout the world.

However, the regulations cannot effectively mitigate social ills without addressing certain obstacles. The heart of the problem is a lack of awareness and understanding of the algorithms that personalize the content presented to users, thereby diminishing personal agency. Currently, the algorithms that target users lack transparency, both to users and to those tasked with addressing social ills. While transparency won't resolve all issues, it is an important step.

ALGORITHM TRANSPARENCY

Social media companies carefully guard the details regarding their data collection practices and targeting algorithms. These are considered proprietary and a matter of competition among social media companies. Without knowledge of how algorithms obtain and utilize collected data to target users, it is difficult to draft effective regulations to tackle issues of data commercialization.

The regulations cited above attempt to increase transparency. The DSA has invested in increasing algorithmic transparency,[13] wherein large online social media companies are expected to implement transparency measures. The DSA designates the European Centre for Algorithmic Transparency (ECAT), to assist in monitoring, testing and analyzing algorithms,[14] although to date ECAT has not published any significant findings regarding social media targeting algorithms. The European Center for Digital Rights has filed over 800 complaints of violations of GDPR—85% of which have not received a decision; approximately 470 of these complaints have been awaiting a decision for more than 1.5 years.[15]

The GDPR and CCPA regulations are more focused on ***data*** transparency. Both pieces of legislation focus on protecting users' rights to their data through mechanisms such as the right to opt out of data collection for information that is not in the public record, the right to know and access collected data, and the right to delete personal information. The GDPR affords users the right to object to their data being processed and the right to correct personal user data. However, since the implementation of GDPR in 2018, there have been over 19,500 complaints and only 37 formal decisions.[16]

The CCPA is the most comprehensive privacy regulation in the United States but it is still in its early stages of implementation. Currently over 360 cases have been filed citing CCPA with approximately 27 percent alleging breaches of data.[17] Some cases have been outright dismissed by California courts. However, some popular social media

AGENCY

What people buy, what they know, and what they believe is increasingly dictated by algorithms that point them to selected content. That content can be misinformation, or intended to capture attention, but is deliberately designed to reduce the user's personal agency in choosing what to view or learn. In this environment, algorithms are increasingly overtaking personal choice and agency in what people read and know.

platforms have adjusted their data collection practices to comply with CCPA. For example, Meta has introduced a new feature for California residents called limited data usage or "LDU." When activated, LDU imposes restrictions on Meta systems to remain compliant with CCPA, providing opt-out options regarding the sale of user data to third-party entities and limiting the collection of certain user data for targeting purposes.

Industry experts widely agree that algorithmic transparency is a necessary step in addressing concerns surrounding social media targeting practices (as well as user literacy and regulatory oversight).[18] With respect to AI algorithms that use machine learning, it is an understanding of the data on which the algorithms are trained that reveals their potential impact.[19] Algorithmic transparency is a prerequisite for regulators to make informed decisions, but true transparency is in its infancy.

FREEDOM OF SPEECH ISSUES

Indeed, even with an understanding of the algorithms, regulation aimed at limiting misinformation may be impeded. In the US, Section 230 (of 47 U.S.C.) states that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[20] The current designation of social media platforms under Section 230 limits the ability of regulators and prosecutors to hold these platforms accountable for the proliferation of misinformation on their platforms. Some experts believe that without Section 230, social media would no longer be a space where users can speak their minds freely without fear of their opinions being removed under the designation of misinformation.[21] These experts fear that if regulation were to place liability on social media platforms for content produced on their sites, these platforms would begin to suppress unpopular opinions, which would have drastic effects on any form of discourse. Other experts believe that Section 230 underestimates the harm that unregulated social media platforms can cause.[22] This disagreement on how to proceed while protecting freedom of speech has left regulators at an impasse.

THE ALGORITHMIC ACCOUNTABILITY ACT

The Algorithmic Accountability Act of 2022 was introduced in the US Senate during the 117th Congress (2021-22) and was tabled in the Commerce Committee. It was reintroduced in the House and Senate during the 118th Congress as H.R. 5628[23] and S. 2892. This proposed legislation would require large technology companies to conduct algorithmic impact assessments and report those findings to the US Federal Trade Commission (FTC), which would then publish an annual anonymized aggregate report.[24] This legislation would represent a step toward increasing algorithmic transparency by specifically focusing on assessing the impact of AI algorithms. However, to date, the bill has not progressed beyond the respective committees.

Even if enacted, mandating self-reporting has proven ineffective in the past, and the FTC currently lacks the technical capabilities to properly determine how this data would be evaluated or analyzed. Algorithmic systems are highly complex and require experts to delineate which ones have a high impact on targeting users and which do not. Aggregate summaries would seem ineffective in properly informing users and the public. Further, although there is discussion of "algorithm governance," it is not practical to regulate an algorithm, which is equivalent to a mathematical proof. Instead, the best that impact assessments can accomplish is a greater understanding of the issues.

The National Institute of Standards and Technology (NIST) could more properly perform algorithmic impact assessments[25] on popular social media platforms. Their analysis could allow regulators (e.g., the FTC) to make informed decisions about social media platforms while preserving technological competition. Within NIST, the Information Science Laboratory has experience with social media research from other projects, with the Software and Systems Division leading projects on the dissemination of information on social media platforms during emergency events. Utilizing NIST would address concerns that trade secrets might become public and that popular social media companies could lose their competitive edge. NIST already has multiple collaborations with private sector entities and creates company-specific agreements through the Technology Partnerships Office. Accordingly, NIST could assemble findings and make salient recommendations to regulators.

WHAT REGULATIONS?

Even with algorithm transparency, it still falls on regulatory bodies and legislative authorizations to enact restraints on data commercialization. To date, the Federal Trade Commission (FTC) has been the primary agency to effect regulations on social media companies. They do this by enforcing privacy standards, and in the future, they might enhance enforcement of opt-out provisions and disclosure of information about how data collections are used in targeted content delivery.

The FTC has taken action against social media companies by imposing fines and mandating privacy program improvements. Their biggest accomplishment to date has been a $5.5 billion fine[26] in 2019 on Meta for privacy violations. Through combined efforts with the Department of Justice, the settlement came with the imposition of new standards of practice that Meta must follow. Other major cases have been brought against Google and YouTube, citing violations relating to data utilization in targeting practices. Through enforcement efforts, the FTC aims to protect consumer privacy and hold prominent social media companies accountable for their breaches of user privacy.

Depending on the impact assessments and discoveries related to algorithm transparency, future regulatory actions are likely to involve opt-out provisions and privacy options, including:

- The right for users to opt out of the sale of personal information;
- The right to restrict or opt out of the use of specific pieces of personal data;
- The right to know and access data that has been collected about oneself;
- The right to delete specific portions of collected data based on history of use of the platform.

While these options prioritize giving users autonomy over data collection and processing, they still allow companies to maintain targeting mechanisms, at least for some users. These changes would empower users to consent to how they want their data shared or used.

Today, companies contend with a patchwork of regulations within the US and throughout the world. The CCPA required

Meta and other social media platforms to include opt-out provisions for the sale of user data, to process user requests for data deletion, to disclose what user content they collect and why, and to include a "Do Not Sell My Personal Information" link on their interface.[27] These changes do not require Meta and other social media platforms to forgo targeting practices, but provide users with the opportunity to impose restrictions. Simultaneously, the GDPR requires all social media platforms obtain strict user consent for data collection along with other privacy mechanisms.[28] Other initiatives seek to ensure media literacy and training. The Digital Citizenship and Media Literacy Act would direct the National Telecommunications and Information Administration to award grants to state and local educational agencies, public libraries, and qualified nonprofit organizations to develop and promote media literacy and digital citizenship education for elementary and secondary school students.[29] Legislation in Washington state provides for teachers to receive training on teaching media literacy,[30] and there is legislation on media literacy in five other states, and media literacy policy in many others.[31]

CONCLUSION

The social media business model incentivizes platforms to maximize user engagement and permits targeted advertising, which can lead to various negative externalities. For US regulation to be effective against complex algorithmic targeting systems, this paper recommends a multifaceted approach to regulation focusing on creating algorithmic transparency, supplemented with media literacy, and mandating opt-out mechanisms on platforms. Through these efforts, the US can effectively shift the incentives surrounding the engagement-first business model and advance the creation of a balanced digital ecosystem for users.

ACKNOWLEDGEMENTS

I would like to thank Dr. Robert Hummel, Mr. Trevor Huffard, Mr. Curtis Pearson, and Dr. Patrick Ennis for their advice and supervision in the production of this paper. I would also like to thank the Potomac Institute of Policy Studies for the opportunity during this past summer to conduct this research. Finally, I would like to thank my parents and brother for their constant love and support.

ENDNOTES

1 "X Privacy Policy." X, 29 September 2023, https://x.com/en/privacy#x-privacy-1.

2 "Meta Privacy Policy - How Meta collects and uses user data." Facebook, 26 June 2024, https://www.facebook.com/privacy/policy/.

3 "Privacy Policy." TikTok, 1 July 2024, https://www.tiktok.com/legal/page/us/privacy-policy/en.

4 Vosoughi, Soroush, et al. "The Spread of True and False News Online." Science, vol. 359, no. 6380, 2018, pp. 1146 - 1151. Science, https://www.science.org/doi/10.1126/science.aap9559.

5 Brewster, Jack, et al. "Beware the 'New Google': TikTok's Search Engine Pumps Toxic Misinformation To Its Young Users." NewsGuard, 14 September 2022, https://www.newsguardtech.com/misinformation-monitor/september-2022/.

6 Pamela Madrid, "USC study reveals the key reason why fake news spreads on social media," Jan 2023, USC Today, https://today.usc.edu/usc-study-reveals-the-key-reason-why-fake-news-spreads-on-social-media/.

7 Agius, Nicola. "Meta's ad revenue jump 24% in Q4, exceeding expectations." Search Engine Land, 1 February 2024, https://searchengineland.com/metas-ad-revenue-q4-2023-437125 .

8 Dencheva, Valentina. "TikTok net ad revenue worldwide 2020-2024." Statista, 20 March 2024, https://www.statista.com/statistics/1344972/tiktok-net-ad-revenue-worldwide/.

9 "Home App Data TikTok Revenue and Usage Statistics (2024)." *Business of Apps*, 8 July 2024, https://www.businessofapps.com/data/tik-tok-statistics/ . Accessed 14 August 2024.

10 Dencheva, Valentina. "Global social media ad spend 2019-2029." *Statista*, 25 July 2024, https://www.statista.com/forecasts/1418549/social-media-ad-spend-worldwide.

11 Ibid.

12 Bittlingmayer, George, and Tyler Cowen. "Advertising." Econlib, https://www.econlib.org/library/Enc/Advertising.html.

13 European Economic and Social Committee, *Digital Services Act and Digital Markets Act – Stepping stones to a level playing field in Europe*, European Economic and Social Committee, 2021, https://data.europa.eu/doi/10.2864/28842.

14 "Questions and answers on the Digital Services Act*." European Commission, 23 February 2024, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348.

15 "5 Years of the GDPR: National Authorities let down European Legislator. 85% of noyb cases not decided." *NOYB*, 23 May 2023, https://noyb.eu/en/5-years-gdpr-national-authorities-let-down-european-legislator.

16 Judgements of the Data Protection Commission, https://www.dataprotection.ie/en/dpc-guidance/law/judgments.

17 "CCPA Litigation Tracker." *Perkins Coie*, https://www.perkinscoie.com/en/ccpa-litigation-tracker.html.

18 Rainie, Lee, and Janna Anderson. "Theme 7: The need grows for algorithmic literacy, transparency and oversight." *Pew Research Center*, 8 February 2017, https://www.pewresearch.org/internet/2017/02/08/theme-7-the-need-grows-for-algorithmic-literacy-transparency-and-oversight/.

19 Rainie, Lee, and Janna Anderson. "Theme 7: The need grows for algorithmic literacy, transparency and oversight." *Pew Research Center*, 8 February 2017, https://www.pewresearch.org/internet/2017/02/08/theme-7-the-need-grows-for-algorithmic-literacy-transparency-and-oversight/.

20 United States, Congress. Section 230, Telecommunications Decency Act, https://www.law.cornell.edu/uscode/text/47/230, 1996.

21 Kelley, Jason. "Section 230 is Good, Actually." *Electronic Frontier Foundation*, 3 December 2020, https://www.eff.org/deeplinks/2020/12/section-230-good-actually.

22 Smith, Michael D., and Marshall Van Alstyne. "It's Time to Update Section 230." *Harvard Business Review*, 12 August 2021, https://hbr.org/2021/08/its-time-to-update-section-230.

23 Text - H.R.5628 - 118th Congress (2023-2024): Algorithmic Accountability Act of 2023 | Congress.gov | Library of Congress.

24 Algorithmic Accountability Act of 2023 Summary (senate.gov).

25 Jacob Metcalf, Emanuel Moss, Elizabeth Anne Watkins, Ranjit Singh, and MadeleineClare Elish. 2021. Algorithmic Impact Assessments and Accountability: The Co-construction of Impacts. InACM Conference on Fairness, Accountability,and Transparency (FAccT '21), March 3–10, 2021, Virtual Event, Canada.ACM, https://dl.acm.org/doi/pdf/10.1145/3442188.3445935.

26 Liu, Henry. "FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook." *Federal Trade Commission*, 24 July 2019, https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook.

27 "United States Regional Privacy Notice | Meta." *Meta Store*, 1 January 2023, https://www.meta.com/legal/united-states/.

28 Wolford, Ben. "What are the GDPR consent requirements?" *GDPR.eu*, https://gdpr.eu/gdpr-consent-requirements/.

29 "All Info - S.394 - 118th Congress (2023-2024): Digital Citizenship and Media Literacy Act." Congress.gov, Library of Congress, 13 February 2023, https://www.congress.gov/bill/118thcongress/senate-bill/394/all-info.

30 Stateline. "Media literacy classes are becoming more popular—but some conservatives see a 'woke' agenda." *Fast Company*, 28 January 2024, https://www.fastcompany.com/91017839/media-literacy-classes-are-becoming-more-popular-but-some-conservatives-see-a-woke-agenda.

31 "Snapshot 2024: The State of Media Literacy Education in the U.S.", National Association for Media Literacy Education, 2024, https://namle.org/wp-content/uploads/2024/01/Snapshot-2024-State-of-Media-Literacy-FINAL.pdf.

Essays and Short Papers

This issue of *STEPS* introduces a section for "Essays" and "Short Papers." These contributions are opinion pieces intended to spark conversation. They are more formal than a blog, but less detailed than a full paper. They are still carefully reviewed and edited. This issue presents two essays, one on Space Debris and another on Government use of AI.

APPROACHING ORBITAL OVERLOAD

Carrie Zuckerman

Carrie Zuckerman previously served as a Research Associate at the Potomac Institute for Policy Studies, through the summer of 2024.

The thousands of satellites orbiting Earth are now integral to our daily lives, essential to communication, navigation, defense, and infrastructure. However, we are increasingly cluttering orbits with human-made debris. At first glance, leaving loose screws, spent rockets, and Tesla Roadsters across the vastness of space might not seem like a problem. Yet, this debris isn't dispersed throughout all of space; it's concentrated in specific orbits around the Earth, which are crucial for our satellite networks. These include orbits used by the International Space Station (ISS), thousands of Starlink internet satellites, and other essential communication satellites. Higher orbits host services we depend on daily, like GPS, weather monitoring, and satellite TV. Our every day lives would change dramatically if satellites in these regions stopped working.

The proliferation of the number of objects in orbit is a recent phenomenon. Access to space has expanded dramatically in the past few decades, allowing more nations and private companies to become spacefaring entities. As a result, orbits are more valuable—and more crowded—than ever before. We've gone from one satellite in 1957 (Sputnik) to nearly 7,000 satellites at the start of 2023 to a predicted 58,000 satellites by the end of 2030.

While this greater access is positive—reflecting Kennedy's assertion that space is for everyone—it also presents risks. More debris is a problem. A runaway cascade of collisions, known as the Kessler Syndrome, could cause destruction of existing satellites and render the most populated orbits unusable. In this nightmare scenario, virtually all air, sea, and land navigation grinds to a halt. Defense systems are incapacitated. The world economy, heavily reliant on time and place stamps, is severely disrupted.

A 2009 NASA study predicted that between 20 and 40 catastrophic collisions were likely to occur in low Earth orbit over the next 200 years, assuming modest increases in satellite launches and the use of strategies to park most objects into safe orbits after their mission ends. The current reality is that these assumptions are too optimistic, and an occurrence of the Kessler Syndrome is inevitable.

Earth orbits are a finite resource whose benefits are accessed by many but owned by none, creating a "tragedy of the commons" scenario. The motivations of individual actors to behave rationally are undermined by the presence (real or imagined) of free-riders and scofflaws. It's a "tragedy" because of the tendency to overuse common resources until they become degraded (e.g., fish stocks, clean air, groundwater).

The UN's 1967 Outer Space Treaty (ratified by 115 countries and signed by an additional 23) holds countries liable for damage caused by their space objects. However, the treaty was not designed with profit-seeking commercial entities in mind, much less multi-national mobile launch platforms that can launch a payload from international waters. The treaty's stipulation that objects in space are the responsibility of the country from which they were launched complicates potential international cleanup efforts.

To date, efforts for technical solutions to address space debris has been limited. For example, the European Space Agency's ClearSpace-1 mission plans to target debris removal in 2026. Ironically, the original anticipated cleanup target recently suffered a collision with—wait for it—space debris.

In recent years, the United States has begun to demonstrate the political will to tackle the space debris problem. In 2022, following a Russian destructive direct assent anti-satellite (ASAT) weapons test, which generated enough new debris to require multiple evasive maneuvers of the ISS, the United States unilaterally pledged not to test this type of ASAT weapon and called for other countries to follow suit. Since then, more countries have joined, with 155 countries voting to approve a (nonbinding) UN resolution discouraging the testing of these weapons. Additionally, in October 2023, the US government levied its first fine on a commercial satellite provider for failing to properly dispose of a dead satellite. That the US should take the lead is more pragmatic than altruistic—the US is responsible for an estimated 30% of all debris and the vast majority of objects in orbit.

Space debris is a tough problem, but international agreements to make progress on "tragedy of the commons" problems are not unknown. In 1987, 197 countries signed the Montreal Protocol, lauded as an exceptionally successful international agreement, and followed through to phase out production of ozone-depleting chemicals. In the 1980s, US Congress levied a tax on chemical and petroleum companies and established a "superfund" to clean up abandoned hazardous sites. More recently, in September 2023, 70 nations and the EU signed a legally binding High Seas Treaty to conserve ocean ecosystems.

Current efforts represent a slow start on the orbital debris issue. Addressing the problem of space debris and sustaining access to the orbital environment will require new and updated international frameworks, adequate collaboration, and realistic resourcing. Space debris is a tough problem, but successful examples in addressing global environmental challenges offer hope and highlight a path forward.

Government Opportunities for AI Technologies

An essay by

Robert Hummel

Chief Scientist, Potomac Institute for Policy Studies

What are we going to do about Artificial Intelligence (AI)?

- The US is in a competition with China for AI “dominance”.
- Companies are pouring billions of dollars into developing AI applications;
- Investors have trillions of dollars of assets in companies producing hardware that supports generative AI;
- Deepfakes have the potential to upend politics, marketing, and individual legacies;
- Artists and others are suing for copyright infringement over AI systems scraping their data; and
- Some worry that after the “singularity,” AI systems will take over and dominate humans!

What a mess! Yet, many believe that AI and its applications, using tools such as large language models (LLMs), are the economic engine for businesses of the future. Applications such as OpenAI’s ChatGPT® and Dall-E® generate billions in revenue, but still lose money due to the immense expense required to create the models.

The government is extremely interested in leveraging AI capabilities and using LLMs. There is a tendency, however, to think that AI offers an alternative to using human intelligence. In actuality, the government’s use of AI technology will still require human input and labor.

Generative models based on LLMs are actually just statistical realizations of models based on a large corpus of training data. Critically, applications depend on large quantities of data, often requiring curation such that only "good" data is used to develop the statistics of normal patterns. Labeling and curation take huge investments in money, compute power, and labor. While companies are in the process of finding commercially viable applications, the government is seeking applications throughout departments and agencies, especially in the Department of Defense, with the hope that the technology can streamline activities to offload labor to technology.

Human labor will still be required, but the kind of labor needed will differ. The AI applications for government can likely accomplish certain tasks with speed and depth beyond human capabilities. Those tasks are the ones that require complex statistical models based on extremely large data sets.

The government is in the enviable position of having access to vast quantities of data. However, that data only has value when analyzed and interpreted. LLMs offer the opportunity to leverage government-collected data to find patterns and develop the statistics to expedite an analysis process. Today, much of the data that the government collects is examined in limited domains by relatively few experts, and much data is left untouched. LLMs can represent the statistics of disparate data sources and discover patterns that have significance. The government has yet to take full advantage of the data that it collects and to utilize LLM technology in applications that provide societal benefit.

There is valid concern that LLM technology be used ethically. Fake imagery, generated misinformation, and mimicked audio tracks are among the ways that LLM technology can be used in divisive and fraudulent ways. Government needs to ensure that it uses the technology ethically and enforces ethical use by the private sector.

Despite the use of the term "intelligence" in the moniker "artificial intelligence," AI does not replace human intelligence with actual intelligence. Rather, LLMs are used to leverage data to recognize patterns that would otherwise be too complex for human observers. However, it is human cognition that must interpret and exploit these patterns by discerning their meaning.

By representing the statistics of normal patterns of data across disparate domains, it should be possible to automate the detection of anomalies in "live" data. This occurs when data either falls outside normal patterns or adheres too closely to a subdomain of data to reflect normal variation. The former can serve as an early warning, while the latter helps discriminate reality versus contrived fakes. In all cases, these applications depend on having built a complex statistical model of "normality" within collected data.

For early warning examples, the government might improve analysis and decision-making processes based on data it collects for the following kinds of applications:

- Early detection of infectious disease outbreaks through analysis of public health data to thwart future epidemics or pandemics;
- Improved forecasting of macro-economic trends in markets to support the Federal Reserve and national economic policies;
- Identification of potential supply chain disruptions and optimized logistics for national needs;
- Early detection of potential geopolitical confrontations, leveraging social media and other data feeds;

- Improved agricultural management through better analysis of multiple environmental data sources—from satellites to road monitors; and
- Diagnostic tools for early warning of medical conditions and insights into best practices for therapies using health data collected by the Centers for Medicare and Medicaid Services (CMS) and other federal agencies, including new sources of data volunteered to these agencies from wearables and monitors.

For discrimination tasks, the government should be able to achieve the following kinds of applications:

- An ability to distinguish data, information, or postings as being "fake" in the sense that they were generated by automated means from a collection of training data; and
- An ability to track the provenance of AI-generated content and expose the sources when content is being appropriated from external sources, whether deliberately or inadvertently.

We can make generated content safe through transparency of its source, so that creative content developed by humans can be appropriately recognized and compensated. Government programs to enable safe AI applications can foster economic growth and innovation.

Development of these applications will be challenging, but requisite technology exists. Much of the effort will involve collecting, managing, aligning, curating, and ingesting data. A particular challenge with early warning applications will be to ensure anonymity and, thus, privacy of the information from individuals that lead to indicators of events. For the discrimination applications, the discriminator must not be used to improve the quality of the fakes, rendering the discrimination application worthless. The challenge will be to limit the availability and stay ahead of the public-sector content generation capabilities by maintaining statistics of a superset of the available training data.

Beyond these application areas, there is a recognition that the fundamental research into statistical modeling is not complete. The capabilities of learning models will continue to improve as further research is conducted. Government needs to ensure that the basic research aspects of machine learning are not frozen at their current state, lest competitors overtake our capabilities in statistical modeling. In the push to attain new and better applications, we need to emphasize the development of the underlying capabilities. and their rapid transition to capabilities.

FEATURED AUTHORS

Robert (Bob) Hummel, PhD

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

Bob Hummel is the Chief Scientist at the Potomac Institute for Policy Studies, the Washington D.C. metro area think tank focused on science and technology issues related to national policies. He is also Editor-in-Chief of STEPS. The Institute supports US government clients and US national S&T policy issues.

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

He is a co-founder of the US Technology Leadership Council, a non-profit industry association. Prior to joining DARPA, he was a tenured university professor at the Courant Institute of Mathematical Sciences at New York University. His area of research is in computer vision and information fusion, publishing in object recognition, image processing, parallel computing, uncertainty reasoning, information fusion, connectionism, and mathematics. He has a PhD in mathematics from the University of Minnesota and a bachelor's degree in mathematics from the University of Chicago.

Rosalie Loewen

Research Economist, Potomac Institute for Policy Studies

Rosalie Loewen works as a Research Economist for the Potomac Institute. Ms. Loewen has broad experience in economic and policy research and analysis with a focus on quantitative methodologies. In the research arena, Ms. Loewen's experience includes work in British Columbia measuring and predicting the effects of new genomics technology uptake. Within the public sphere, Ms. Loewen was privileged to serve two overseas tours with the US government as a diplomatic officer. Ms. Loewen spent her early career in the private sector, in finance, as a mergers & acquisitions analyst with a focus on modelling net present value. Ms. Loewen holds a master's degree in Economics from the University of British Columbia, a master's degree in International Relations from Johns Hopkins' SAIS, and a bachelor's degree from Harvard College.

Alden V. Munson, Jr.

Senior Fellow, Member Board of Regents
Potomac Institute for Policy Studies

Mr. Munson is a Senior Fellow and Member, Board of Regents at Potomac Institute for Policy Studies. He is an advisor to the US intelligence and defense agencies and to industry, and is a member of the Board of SMA, a competition management and consulting company. He is an active member of the Intelligence and National Security Alliance (INSA) and the US GEOINT Foundation (USGIF).

He served on the Defense Science Board and contributed to studies in cloud computing, cyber resiliency, electronic warfare, space resiliency and long-range strike, among others, and has participated in Air Force Studies Board activities on digitization of the Air Force.

He was the Deputy Director of National Intelligence for Acquisition and Technology from May 2007 until July 2009. Previously he was a consultant in defense, space, and intelligence and was associated with the investment banking firm Windsor Group.

He was Senior Vice President and Group Executive of the Litton Information Systems Group, leading information technology, command and control, and intelligence businesses for defense, intelligence, civil, commercial, and international customers. Mr. Munson was Vice President at TRW, in the System Integration Group, the Space and Electronics Group, and the Information Systems Group (the former TRW Credit Business). In these assignments, he led numerous space, intelligence, and information technology organizations and activities. He began his career at the Aerospace Corporation, where he provided system engineering support to many space and intelligence programs.

Mr. Munson received a bachelor's degree in mechanical engineering from San Jose State University and a master's degree in mechanical engineering from the University of California, Berkeley. The National Reconnaissance Office named Mr. Munson as a Pioneer of National Reconnaissance, and received the National Intelligence Distinguished Service Medal in 2009.

Carrie Zuckerman

Research Associate, Potomac Institute for Policy Studies

Carrie Zuckerman served as a Research Associate at the Potomac Institute for Policy Studies when the essay in this issue was researched and written. At the Institute, Carrie focused on space policy issues for customers including NASA and Space Force. Prior to joining the Institute, she received a bachelor's degree in political science and a minor in astrophysics at the University of California Berkeley. While at Berkeley, she contributed to astrophysics research focused on improving ground-based exoplanet imaging.

Kayla Dunn

Intern, Potomac Institute for Policy Studies

Kayla Dunn is a senior at Georgetown University where she is majoring in Science, Technology and International Affairs with a focus in Business, Growth and Development. In 2024, she completed the Potomac Institute S&T Internship program, where she investigated algorithmic targeting on social media platforms. Motivated by an interest in science policy, Kayla plans to pursue a Masters Degree after graduation in Data Science and Applied Analytics, where she hopes to leverage her understanding of the data systems and data analytics to strengthen her advocacy and research efforts.

STEPS (Print) ISSN 2333-3219
STEPS (Online) ISSN 2333-3200