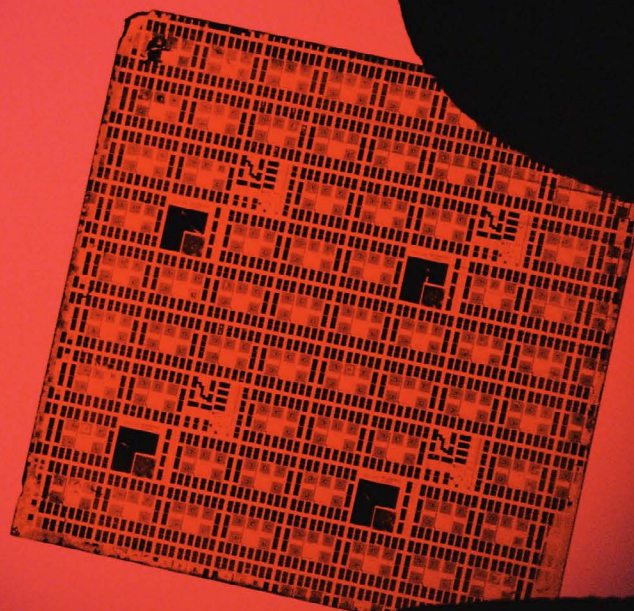


EMBARGOED

Regaining the Digital Advantage: A Demand-Focused Strategy for US Microelectronics Competitiveness

BRYAN CLARK AND DAN PATT

CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY, HUDSON INSTITUTE



© 2021 Hudson Institute, Inc. All rights reserved.

ABOUT HUDSON INSTITUTE

Hudson Institute is a research organization promoting American leadership and global engagement for a secure, free, and prosperous future.

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson seeks to guide public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings and recommendations.

Visit www.hudson.org for more information.

Hudson Institute
1201 Pennsylvania Avenue, N.W.
Fourth Floor
Washington, D.C. 20004

+1.202.974.2400
info@hudson.org
www.hudson.org

Cover: Light reflects through an integrated circuit. (Lawrence Manning/Getty Images)

Regaining the Digital Advantage: A Demand-Focused Strategy for US Microelectronics Competitiveness

BRYAN CLARK AND DAN PATT

CENTER FOR DEFENSE CONCEPTS AND TECHNOLOGY, HUDSON INSTITUTE



ABOUT THE AUTHORS

Bryan Clark

Senior Fellow and Director, Center for Defense Concepts and Technology

Before joining Hudson Institute, Bryan Clark was a senior fellow at the Center for Strategic and Budgetary Assessments (CSBA) where he led studies for the Department of Defense Office of Net Assessment, Office of the Secretary of Defense, and Defense Advanced Research Projects Agency on new technologies and the future of warfare. Prior to joining CSBA in 2013, Mr. Clark was special assistant to the chief of naval operations and director of his Commander's Action Group, where he led development of Navy strategy and implemented new initiatives in electromagnetic spectrum operations, undersea warfare, expeditionary operations, and personnel and readiness management. Mr. Clark served in the Navy headquarters staff from 2004 to 2011, leading studies in the Assessment Division and participating in the 2006 and 2010 Quadrennial Defense Reviews. Prior to retiring from the Navy in 2008, Mr. Clark was an enlisted and officer submariner, serving in afloat and ashore submarine operational and training assignments, including tours as chief engineer and operations officer at the Navy's Nuclear Power Training Unit.

Dan Patt

Adjunct Fellow, Center for Defense Concepts and Technology

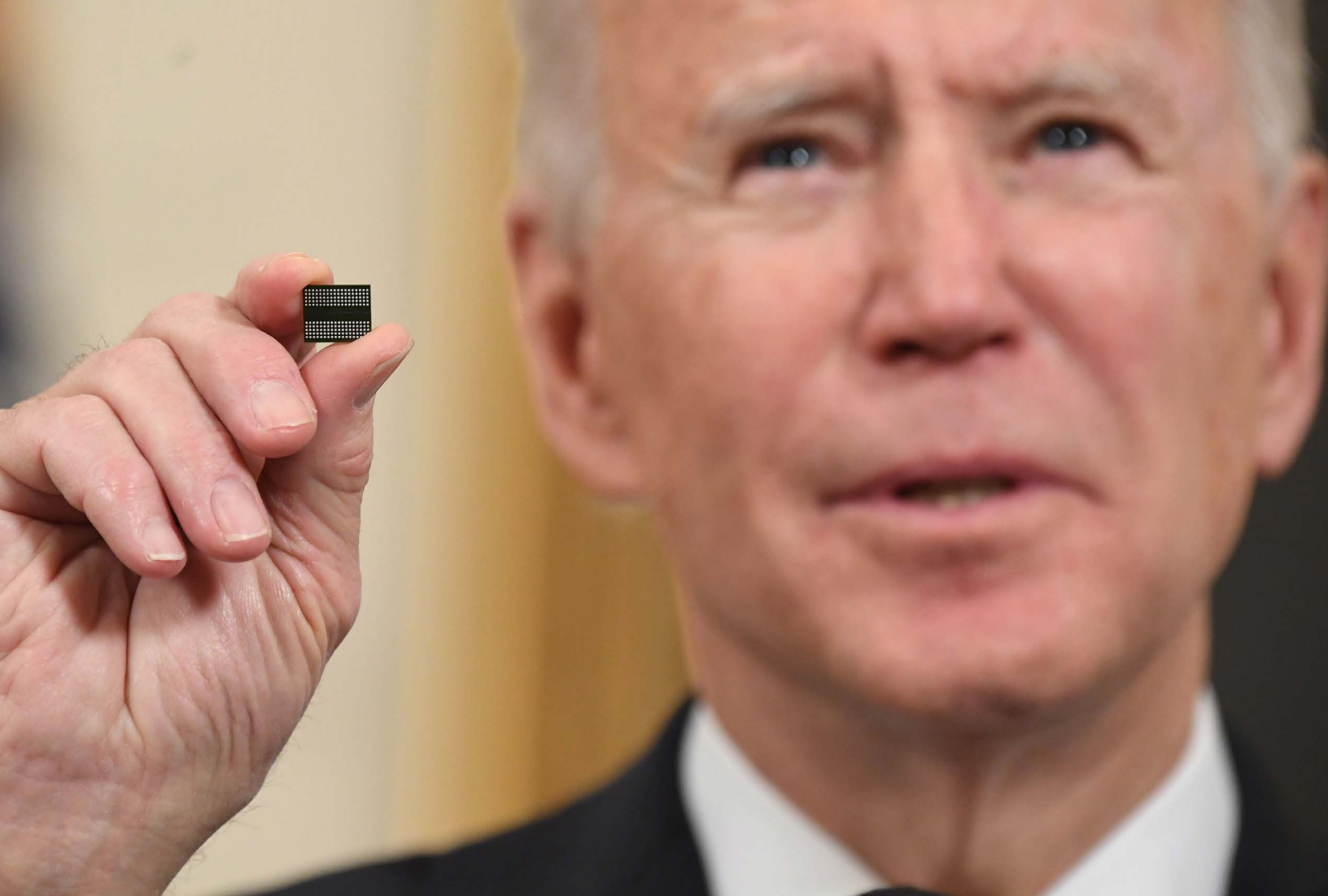
Dan Patt focuses on the role of information and innovation in national security in his work at Hudson. Dr. Patt supports strategy at the artificial intelligence company **STR** and supports Thomas H. Lee Partners automation fund. He has more than fifteen years' experience operationalizing emerging technology including artificial intelligence, networked information systems, robotics, supply chain automation, and enterprise information technology. Dr. Patt also served as deputy director for the Defense Advanced Research Projects Agency's (DARPA) Strategic Technology Office (STO), managing more than \$400 million in annual technology investments in robust distributed systems architectures in a technology portfolio including battle management, command and control; communications and networking; intelligence, surveillance and reconnaissance; and electronic warfare. At DARPA he launched the Mosaic Warfare initiative. Dr. Patt received his B.A., M.S., and Ph.D. in aerospace engineering from the University of Michigan.

The Center for Defense Concepts and Technology at Hudson Institute

Hudson Institute's Center for Defense Concepts and Technology examines the evolving field of military competition and the implications of emerging technologies for defense strategy, military operations, capability development, and acquisition. The center focuses on a comprehensive view: connecting strategy with new operational concepts; assessing the weapons and systems needed to implement new concepts; and evaluating the necessary commitment of resources.

TABLE OF CONTENTS

Chapter 1. Introduction	7
Concentration—Not Globalization—Threatens the US Microelectronics Supply	8
Chapter 2. Tiny Building Blocks of the Modern World	10
The Rise of Fabless Manufacturing	13
Disaggregation and Threats to Supply Chain Reliability and Security	15
Simplistic Solutions Based on a Simplistic Model	16
Chapter 3. A Framework for the Microelectronics Ecosystem	17
Four Key Factors with Which to Assess the Microelectronics Ecosystem	18
Moving Up the Value Chain	23
Chapter 4. Applying the Framework	27
Assessing the Microelectronics Ecosystem from the US Perspective	28
Evaluating Potential Solutions	30
A Framework for Decision-Making	36
Chapter 5. A Strategy for Increasing Resilience, Assurance, and Competitiveness	37
Endnotes	40



CHAPTER 1. INTRODUCTION

The microelectronics industry plays an outsized role in America's commercial and civic life. Although computers and electronic equipment only make up about 2 percent of US domestic output, they host financial and professional services that form half of the US economy and provide the brains for nearly every durable consumer product and military system.¹ Microprocessors are also a critical element of national infrastructure, as they manage all of America's energy grids, transportation systems, and telecommunications networks. Without a reliable supply of computer chips and microelectronic components, most US economic and societal activity would eventually grind to a halt.

The increasing reliance of products and services on microelectronics was brought into stark relief during 2021. Due to high capital costs and long lead times for new facilities, semiconductor supply chains were unable to quickly expand

output or change their product lines to meet rising orders as economies recovered from the COVID-19 pandemic. The resulting chip shortages slowed delivery of finished goods ranging from automobiles and refrigerators to video game consoles and medical devices; supplies are not expected to meet demand until 2022.²

To address the current chip shortfall, advocates renewed longstanding calls for federal support to expand US semiconductor fabrication, which fell from nearly 40 percent in 1990 to just 12 percent of global production in 2020.³ These

Photo caption: US President Joe Biden holds a microchip as he speaks before signing an executive order on securing critical supply chains in the State Dining Room of the White House in Washington, DC, February 24, 2021. (Saul Loeb/AFP via Getty Images)

efforts, however, are trying to solve the wrong problem and could misallocate government funding to uncompetitive facilities while failing to invest in the computing and manufacturing technology that will improve US microelectronics resilience, assurance, and competitiveness for the long-term.

Concentration—Not Globalization—Threatens the US Microelectronics Supply

Rather than representing flawed industrial policy, shrinking US semiconductor production merely reflects the microelectronics industry's disaggregation in response to market forces that incentive manufacturers to outsource some production steps to specialists which can achieve lower cost and higher performance using their expertise and local government support. And even though most US-based microelectronics companies now fabricate their chips overseas, the United States remains the global semiconductor market leader, responsible for more than 45 percent of sales by value.⁴ US semiconductor companies' reliance on international suppliers resembles that of such US-based industrial champions as top-10 global carmakers Ford and General Motors, both of which average only 40% of domestically sourced content in their vehicles.⁵

The disaggregation of US microelectronics production away from *integrated device manufacturers* (IDMs) like Intel is therefore a predictable evolution and does not necessarily represent a reduction in the resilience of US semiconductor supplies. On the contrary, today's US semiconductor shortages arguably result from microelectronics production being too concentrated. Although the chipmaking process is now spread across multiple companies and continents, each step in the supply chain is dominated by a few firms that have rationalized their capacity to meet current demand. As a result, localized disruptions have an outsized impact on overall output.

Fabrication is the most prominent example of semiconductor supply chain concentration. During the last 30 years, foundries located in Taiwan and South Korea displaced US, Japanese,

and European IDMs to become market leaders in chip-making thanks to a combination of low regulatory costs, generous government grants, and tax breaks.⁶ Because fabrication plants cost billions of dollars to build and require frequent upgrades thereafter, countries having more highly diversified economies chose not to invest in national champion chipmakers. Consequently, more than 70 percent of world semiconductor fabrication is now concentrated with Taiwan Semiconductor Manufacturing Company (TSMC) and South Korea's Samsung.⁷

Supporters of subsidizing US chip fabrication also argue that overseas foundries create a risk that security vulnerabilities could be incorporated into microelectronics during fabrication or packaging.⁸ Even though domestic foundries could increase ease of oversight, the most significant of recently reported semiconductor security flaws were introduced during chip design.⁹ Instead, the more important impact of the disaggregated microelectronics supply chain is that the resulting concentration leaves customers with few options to shift production when security concerns arise at a particular foundry.

Using government investment to bring more steps of the microelectronics production and assembly process onto US shores could help diversify the semiconductor supply chain and thereby improve resilience and assurance. However, without ongoing subsidies, US foundries may be unable to compete with TSMC or Samsung in affordably building the most sophisticated chips. Moreover, US partners and allies could be more effective hosts for new foundries if they have lower costs and a greater willingness to provide ongoing financial and regulatory support to national champion fabrication firms.¹⁰

Instead of reacting to temporary chip shortages or potential security vulnerabilities by reflexively onshoring the microelectronics supply chain's costliest elements, the focus of government interventions should be policy changes or investments that would provide the greatest leverage in improving US microelectronics competitiveness, resilience,

and assurance today and over the long-term. This study is intended to inform these decisions by providing a framework for assessing the microelectronics supply chain and evaluating government actions by objectively considering both sides of the microelectronics ecosystem—supply and demand.

This study's proposed framework suggests the US government has a historic opportunity to strengthen and secure the US microelectronics ecosystem by adopting a two-pronged policy and investment strategy using authorities granted by the 2021 National Defense Authorization Act (NDAA) and funding from proposed legislation designed to improve US competitiveness.¹¹ These Congressional actions, however, are weighted toward production of today's IC technologies in which US fabrication and packaging are small players, rather than research and development (R&D) of future architectures where the US microelectronics industry could gain an enduring advantage.

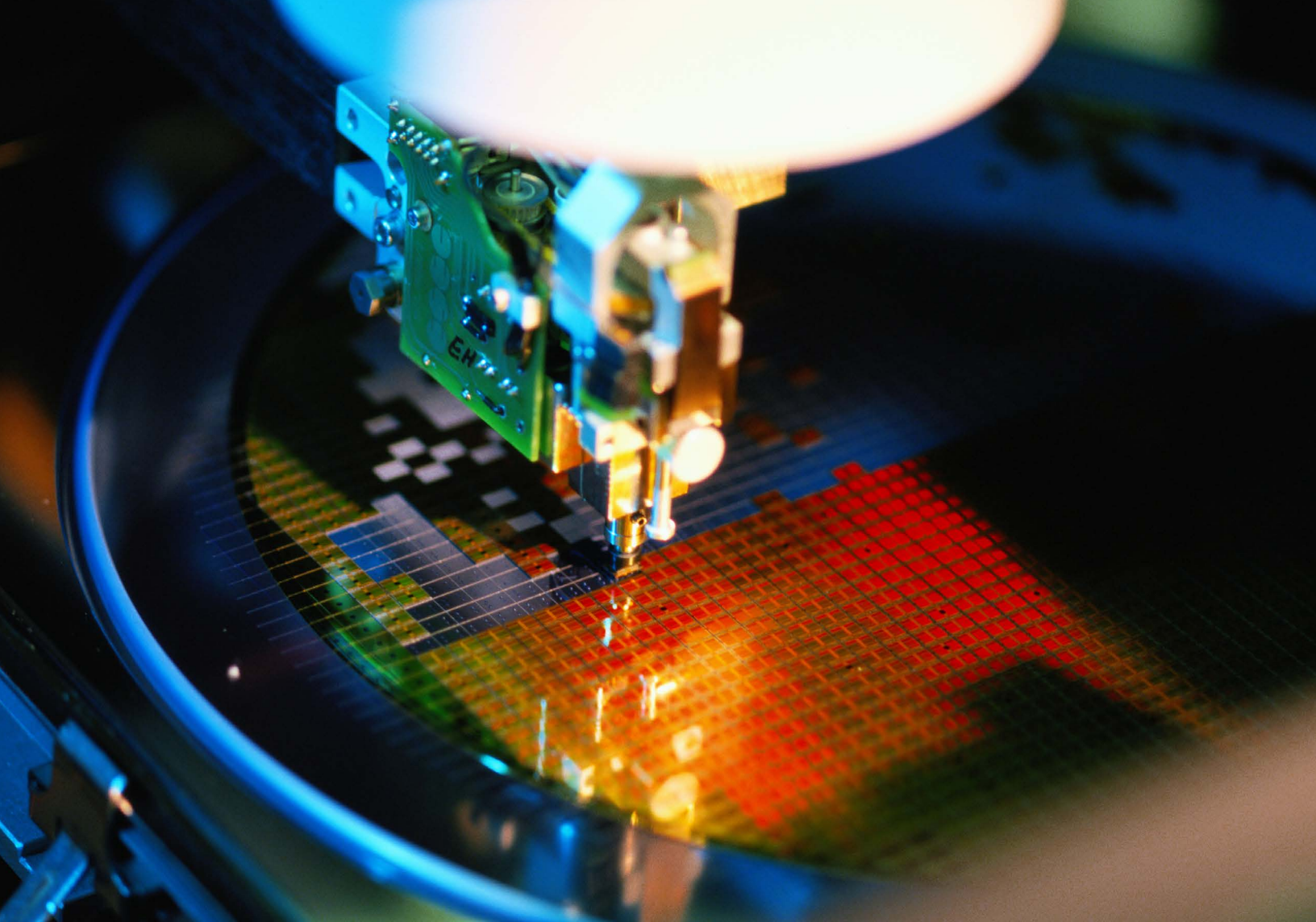
The strategy's first line of effort would invest in the US microelectronics industry's future to provide it an advantage over foreign competitors by exploiting the emerging transition in chip design from simply increasing density to growing complexity and specialization in architecture and design. By focusing federal microelectronics investment on R&D of future IC technologies and manufacturing processes rather than production of today's chips, the US government could improve semiconductor supply resilience and assurance while restoring the US semiconductor producers to a competitive position across each segment of the supply chain.

To achieve these goals, however, government R&D investment cannot be limited to basic research but must also be used to bridge new microelectronics technologies through applied research to commercialization. Whereas the US government has long invested in technology development, commercialization

depends on an understanding of market demand, necessitating new mechanisms to guide government spending. Co-investing with US industry players through constructs such as public-private partnerships (PPP), built in the mold of SemaTech or In-Q-Tel, are a proven means of getting next generation technology to market. Government sponsors can provide an investment base that reduces risk to private investors while also shaping investment decisions to reflect government concerns and interests like security or operational utility. The PPP can consider market demands and weigh the balance of investment between infrastructure and product in an agile fashion.

To enable the strategy's main effort, its second prong calls for modest government funding to catalyze greater diversity in production of today's generation of chips, which would improve supply chain resilience and assurance and grow the fabrication and packaging capacity needed for future IC technologies. This line of effort would encourage market leaders TSMC or Samsung to build more US facilities in partnership with American firms and spur US companies like Global Foundries and Intel to expand domestic production by mitigating the higher cost of US operations through a combination of tax and regulatory incentives.

Government funding in the strategy's second prong would not be used for building and outfitting new plants but would instead focus on closing the operating cost differential between US and overseas production. As a result, the business case for new facilities would be improved, which could unlock private funding for facility construction and equipment. To further diversify microelectronics production, the strategy would employ purchase agreements, export controls, and technology sharing with US allies to encourage them to also host new fabrication and packaging capacity and help build a demand alliance that would counter China's desire to grow its industry's power in international markets.



CHAPTER 2. TINY BUILDING BLOCKS OF THE MODERN WORLD

Integrated circuits (IC) are the most important elements in any microelectronic system, where they manage power supplies, store programs and data, sense the environment, and process data. At its most fundamental level, an integrated circuit (IC) is a collection of transistors created by joining two layers of semiconductor material. To enhance their ability to carry electrical current, one layer is doped with a metal having free electrons in its outer shell, and the other is doped with a metal having open positions in its outer electron shell.¹² The right amount and type of doping ensures that the difference in energy levels between the free electrons and the holes is sufficiently narrow that application of a small voltage causes electrons to jump from one layer to the other, thus generating a current and forming a transistor.

In an analog IC, the transistor's output current is varied continuously by varying the voltage applied to its layers, essentially making it an amplifier. Once the only form of IC, analog semiconductors are now used primarily in applications requiring variable output to reflect voltage input, such as photovoltaic cells, light-emitting diodes, and power-management systems.¹³ Analog ICs can also support high-voltage applications such as radars or amplifiers, in part by using semiconducting materials other than CMOS, such as gallium-arsenide and gallium-nitride (GaN).

Photo caption: An integrated circuit being manufactured on a silicon wafer. (Yellow Dog Productions/Getty Images)

In contrast to analog circuits, digital ICs use transistors as on-off switches. Digital ICs are mostly composed of silicon-based *complementary mixed-oxide semiconductors* (CMOS), because their relatively smaller band gap reduces power requirements and heat generation. For the current generation of digital IC designs, processing speed or storage capacity correlates positively with circuit density. Today, the features, or nodes, that carry electricity in an IC are only 7 to 100 nanometers wide, requiring that chipmakers use lasers to etch circuits onto silicon wafers. By shrinking the laser's wavelength, millions of transistors can fit on a memory chip able to store gigabits of information or a microprocessor capable of performing billions of calculations per second. According to Moore's Law, circuit density and thus performance are expected to double approximately every 18 months, although the difficulty of etching ever smaller circuits and dissipating the heat they generate is beginning to constrain IC performance.¹⁴

A relatively small variety of architectures are used in memory chips. Static random-access memory (SRAM) chips can store large amounts of data and achieve the rapid transfer rates needed for applications like a video cache, whereas slower and less-expensive dynamic RAM (DRAM) chips are used to hold the data and programs currently in use by a microprocessor. Flash memory and electrically-erasable programmable read-only memory (EE PROM) ICs provide greater permanence compared to RAM for long-term storage. Give their narrow range of designs, memory IC manufacturers compete primarily on performance, and thus node size, resulting in the half-dozen companies able to build very dense ICs controlling more than 80 percent of the memory chip market.¹⁵

Unlike memory ICs, manufacturers produce microprocessors in a wide diversity of architectures from simple circuits for rote functions like timing or controlling vehicle emissions to the extremely sophisticated central processing units (CPUs) or graphics processing units (GPUs) used in computers and gaming consoles. Although capable of supporting a variety of

functions, some CPUs and GPUs are specifically designed to efficiently run particular operating systems and work with specific computer hardware, such as the M1 chip used in Apple's new MacBook computers.¹⁶ A new generation of IC architectures is also emerging that combine elements of CPUs, GPUs, and memory to support the unique information flows required for effective artificial intelligence (AI)-enabled operations.¹⁷

Although highly versatile, CPUs and GPUs are not the best microprocessors for all situations. *Application-specific integrated circuits* (ASICs) are built to provide a narrow set of characteristics that yield optimal performance in particular use cases, often hosting tailor-made software. Although their specialization generally makes ASICs more expensive than CPUs or GPUs, they can be more affordable when purchased in large quantities. In contrast to general CPUs, ASICs can provide critical performance advantages by only incorporating those design elements needed for them to perform their intended function. ASICs are often used in digital signal processors or the control systems of medical devices, home appliances, and automobiles, where power efficiency, low latency, and reliability are priorities.¹⁸

The other main type of specialized microprocessor is the *field programmable gate array* (FPGA). Whereas an ASIC is designed with a particular architecture, FPGAs allow the component manufacturer to configure the circuit's transistor arrays with software before use. Because their physical design is not specialized, tailoring FPGAs to fit specific applications is less expensive than creating ASICs to do so, but FPGAs must be reprogrammed to support each new use.¹⁹

Efforts to improve CMOS IC speed or capacity by reducing feature size are approaching physical and manufacturing limits. To continue increasing performance, chipmakers are beginning to pursue more disaggregated chip designs, such as *systems on a chip* (SoC) that combine multiple ICs into a single package and *systems in a package* (SiP) that integrate CMOS and

Figure 1: Comparison of microprocessor (digital logic chip) types

TYPES OF MICROPROCESSORS				
	CPU	GPU	FPGA	ASIC
Compute adaptability	High	Medium	Low	None
Compute power	Medium	High	High	Medium
Latency	Medium	High	Low	Ultra-low
Throughput	Low	High	High	High
Parallelism	Low	High	High	High
Power efficiency	Medium	Low	Medium	High

Source: Authors; based on Arnon Shimoni, "A gentle introduction to hardware accelerated data processing," Hackernoon.com, August 27, 2018, <https://hackernoon.com/a-gentle-introduction-to-hardware-accelerated-data-processing-81ac79c2105>.

non-CMOS ICs.²⁰ In many existing microelectronics designs, memory chips and microprocessors are separate and mounted on circuit boards to enable different system configurations and allow various suppliers to provide ICs for a system. However, this architectural approach introduces latency due to the distance between components. In an SoC, all the ICs for an application are combined within a single chip, reducing the distances between them and enabling a wider variety of architectures. Although SoCs can be built from a set of complete ICs, the SoC approach allows the use of partial ICs or “chiplets” that may not include all the features of a stand-alone chip and which are attached to a common substrate or physically stacked onto one another to form complete 2.5D or 3D circuits.²¹ The customization possible with an SoC is similar in intent to an ASIC, but an SoC can mix commodity and specialized chip types, thus opening up a design space for lower-cost solutions compared to an ASIC.²²

Although IC performance is improving much faster than that of other products, the microelectronics industry is also very mature. Like other mature manufacturing sectors, older IC designs and architectures are still in wide use and continue to

be produced by more companies than are building the most sophisticated chips with the smallest node sizes. For example, the chips shortages being experienced in the aftermath of the COVID-19 pandemic are most acute among the legacy, large-node semiconductors that have replaced many of the analog electrical control systems in appliances and vehicles.

The production process for old and new semiconductors evolved in response to market forces. Semiconductor manufacturers and service providers thrived in locations with local expertise and low costs for labor, regulatory compliance, and utilities, as well as robust government financial support in the form of subsidies or tax reduction. Improved shipping efficiency and management encouraged specialization by lowering the cost to move products between steps of an industrial process.²³ As a result, before most chips are installed in mobile phones or other consumer electronics, they and their constituent raw materials will have passed through a dozen or more companies located on two to three continents. Thanks to real-time data analysis and dependable shipping, global microelectronics production is now optimized to deliver components just in time for the chain’s next step.²⁴

The Rise of Fabless Manufacturing

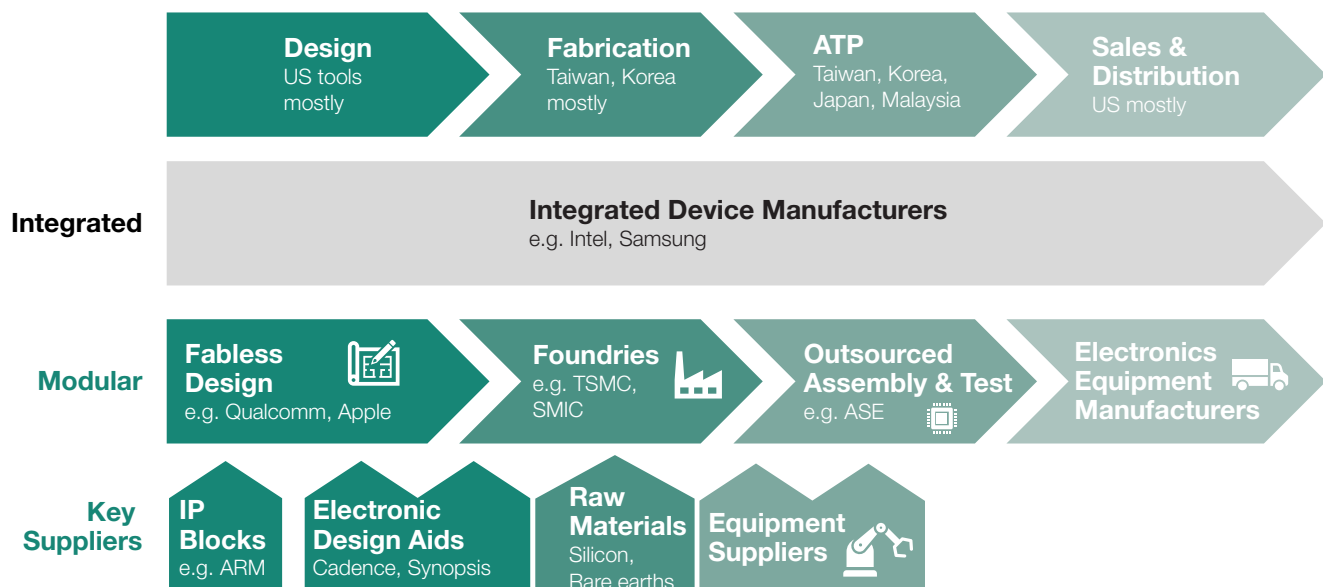
Microelectronics manufacture was not always globalized. During the rise of personal computing in the late 20th Century, America's Intel was the predominant supplier of PC microprocessors, building CPUs for market leader IBM as well as upstart competitors Dell, Compaq, and Hewlett-Packard. Although it relied on overseas companies for raw materials and some manufacturing equipment, as an IDM Intel created the chip architecture and design in addition to conducting every step of the production and sales process.²⁵

Intel's dominance in the consumer CPU market began to erode with the rise of mobile devices and the emergence of new manufacturers that specialized in parts of the IC production process, particularly those where they could integrate horizontally

to achieve efficiencies and lower costs than an IDM.²⁶ The advent of specialized chip foundries like AT&T, LSI Logic and VLSI Technology made possible *fabless chip manufacturing*, in which a company designs its own chips which a foundry builds under contract. The availability of electronic design automation (EDA) tools built by software makers like US-based Cadence and Synopsis further spurred expansion of the fabless model.

Fabless manufacturing has been used for decades by American chipmakers including Broadcom, Nvidia and Qualcomm.²⁷ Apple joined the ranks of fabless manufacturers in 2017 with its A11 mobile phone microprocessor, which was joined in 2020 by the M1 CPU for laptops and tablets.²⁸ And in a major capitulation to the fabless trend, Intel announced in 2021 it would use overseas foundries to build some of its chips

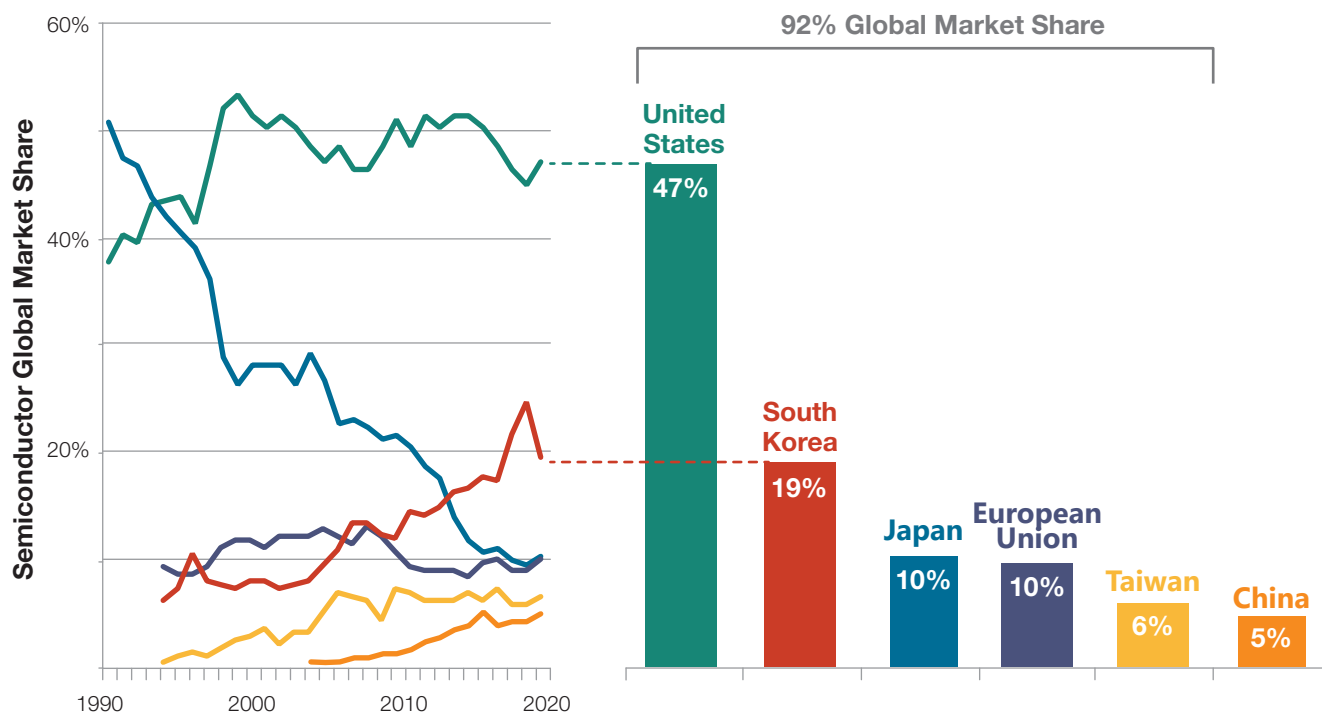
Figure 2: The semiconductor supply chain



Microelectronics manufacturers produce semiconductors and assemble them into finished circuits and modules for customers to incorporate into their systems.

Source: Authors

Figure 3: Semiconductor global market share by country (1990-2020)



US companies dominate the global market share in semiconductors, even as lower value-added functions of fabrication, packaging, and assembly have shifted overseas. China has only captured 5% of the global market despite tremendous investment.

Source: "2020 State of the US Semiconductor Industry," Semiconductor Industry Association, June 2020, <https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf>.

after failing to achieve state-of-the-art node sizes in its own fabrication facilities.²⁹

Free to focus only on building ICs that other companies design, foundries compete primarily on price and node size. Each move toward smaller features costs more to create, build, and execute, but yields higher performance increases per unit cost compared to the previous generation. Through technology investments and close relationships with the leading US fabless manufacturers Samsung and TSMC steadily gained market share and eventually dominated semiconductor fabrication. Today, TSMC and

Samsung make 70 percent of contracted chips overall and all the highest-performing chips that have node sizes of less than 7 nm.³⁰

Specialization has also extended to other steps of the IC production process. Samsung and TSMC depend on Dutch firm ASML for the extreme ultraviolet (EUV) light etching machines needed to create the small features in high-end chips.³¹ To reduce costs and overhead, foundries also outsource the *assembly, test, and packaging* (ATP) process of cutting etched silicon wafers into chips and preparing them to be installed in a customer's systems.

Despite semiconductor manufacturing's disaggregation, US companies still lead the global chip market due to their strengths in design and sales. As shown in Figure 3, US semiconductor market share remained above 40 percent and rose during the past 30 years, largely at the expense of Japanese chipmakers. The United States has sustained its lead in semiconductor sales by embracing rather than resisting globalization because, while Intel remains an IDM, most other US chip suppliers employ a fabless model for all or some of their products.

In addition to prompting concentration, specialization in semiconductor production initiated a race to the bottom among service providers and fabricators with respect to price that—along

with government subsidies in some cases—has reduced profit margins and now dissuades competitors from entering the market. This barrier to entry is most challenging for chip fabrication plants, which cost about \$4 billion to construct and equip for the manufacture of ASICs like those used in vehicles and medical devices and more than \$15 billion to produce the latest GPUs or CPUs.³²

Disaggregation and Threats to Supply Chain Reliability and Security

The semiconductor industry, like other commodity-based industries driven by a relentless push for efficiency, periodically suffers supply chain disruption when production capacity is lost or customer demands change. The COVID-19 pandemic

Figure 4: Geographical distribution of the semiconductor supply chain



Today, the semiconductor supply chain is widely distributed, with a product passing through many different geographic locations before reaching its final destination. The geographic concentration of many elements in Asia constitutes a geopolitical concern. Establishment of US foundries cannot, by itself, solve global resilience issues, and alliance-based approaches are required to increase resilience in the semiconductor supply chain.

Source: Authors

combined with the considerable increase of semiconductor content in most every durable product caused a greater than normal supply chain disruption during 2021.³³ Although today's shortages resulted in part from a global health crisis, the next disruption could be geopolitical. As shown in Figure 4, most steps in semiconductor manufacturing are concentrated in East Asia, where they could be subjected to pressure or coercion by the government of the People's Republic of China (PRC) or become geographically isolated from US designers and customers were shipping networks to break down.

Disaggregation of microelectronics supply chains also raises concerns among manufacturers and customers that their chips have been constructed as intended and as advertised and are free of security vulnerabilities. Although fabless semiconductor companies design their own ICs, outsourcing fabrication, packaging, and testing in the United States or overseas could increase opportunities for the introduction of inadvertent bugs, flaws, or intentional back doors, which hackers could use to access or turn off a circuit.³⁴ Such security vulnerabilities are of greatest concern in chips destined for national security applications such as controls for critical infrastructure or weapons systems purchased by the US Department of Defense (DoD).³⁵

To assure their microelectronics are free of bugs and back doors, fabless companies employ extensive quality control measures during and after manufacture.³⁶ However, threats to semiconductor security will likely grow as chip lifecycles lengthen, increasing the time hackers have to find and exploit potential vulnerabilities and develop attacks. Potentially the most important impact of supply chain disaggregation on assurance is that even if testing and oversight are effective, concentration of microelectronics production with a few manufacturers reduces customer options in choosing an IC supplier and may preclude switching suppliers to address a security concern. Partly to improve assurance, the US government authorized in 2020, but has not yet appropriated, funding to support construction of more semiconductor fabrication facilities in the United States.³⁷

Simplistic Solutions Based on a Simplistic Model

Although questions about microelectronics availability and security are legitimate, the answers proposed by the US government and industry to date are based on a simplistic supply chain model that fails to account for demand and the increasing technological complexity of microelectronics. Rather than developing in isolation, today's microelectronics supply chain configuration is a response to dynamic market forces exerted by current and prospective customers. The microelectronics supply chain could therefore be more properly characterized as the *microelectronics ecosystem*.

As evidenced by recent government action and calls from the semiconductor industry, the most prominent initiative being pursued to improve resilience of and customer assurance in microelectronics production is public subsidies for US chip fabrication.³⁸ However, this one-size-fits-all solution does not necessarily secure US microelectronics manufacture, which can accrue security vulnerabilities throughout the production cycle, whether located in the United States itself or elsewhere. Onshoring fabrication also fails to account for current and future demand, which could render new US-based fabrication facilities uncompetitive or technologically obsolete and therefore unable to ensure chip supplies. A more comprehensive approach is needed to better assess the microelectronics ecosystem in order to develop approaches to increase its resilience and its assurance for US customers.

The framework proposed within this study, which is based on a more thorough evaluation of the microelectronics ecosystem, incorporates its wide variety of elements and relationships, the influence of today's semiconductor market, and the importance of adding value to support future demand. In addition to enabling improved risk assessments of the current supply chain, the proposed framework enables a more realistic evaluation of potential government policies or investments in preventing future chip vulnerabilities or shortages, while positioning US chipmakers to become more competitive in the global microelectronics market.



CHAPTER 3. A FRAMEWORK FOR THE MICROELECTRONICS ECOSYSTEM

Most models of the microelectronics supply ecosystem include only the supply-side contributions of product and service providers.³⁹ In relatively stable industries such as automobile or appliance manufacturing, supply chain assessments may be sufficient to inform effective government policies. In comparison to these industries, however, the microelectronics market is more dynamic, with fresh IC designs and software architectures emerging nearly continuously in response to new use cases, security liabilities, or the need to provide additional value for prospective customers.



In the microelectronics ecosystem, supply-side solutions are likely to eliminate only temporarily an IC shortage, close off one

class of security vulnerability, or prop up a US semiconductor supplier for the near-term. To provide more enduring solutions, US government interventions should consider current and future demand to assess whether government interventions are likely to be sustainable and produce their desired effects.⁴⁰

To guide government policies and investments that promote security, semiconductor availability, and increased US competitiveness, this study proposes a framework comprising four factors, measured from the perspective of the US microelectronics

Photo caption: An engineer uses a digital tablet for quality inspection in an automated production line. (Nitat Termmee/Getty Images)

Figure 5: Factors addressed in the proposed microelectronics ecosystem assessment framework

 RESILIENCE	 ASSURANCE	 DEMAND	 NEW VALUE
Definition: Can US customers (consumers and DOD) reliably receive materials and equipment?	Definition: Can vulnerabilities and exploits be introduced that would not be detected in testing?	Definition: Is there a market for US players in current and near-term tech, as driven by (largely commercial) global demand.	Definition: How can US companies be leaders in next-generation technologies?
Opportunity: Achieving a microelectronics supply that is resilient to Chinese influence, war, natural disaster, or capricious government policy	Opportunity: Confidence that microelectronics components are free from exploits and vulnerability	Opportunity: Meeting and harnessing near-term global market demand for microelectronics, and the healthy businesses and economic activity that accompany it	Opportunity: Producing new and emerging technologies that will address future market demand, creating new virtuous cycles of industry

Source: Authors

customers and industry: resilience of continued microelectronics supplies to the US market; assurance that US microelectronics reflect their intended design and are free of security vulnerabilities; the ability of the US microelectronics industry to meet current microelectronics demand, which shapes the ecosystem; and the value added from US firms, which supports future demand. Assessing each element of the current microelectronics supply chain through these four lenses can highlight priority areas for US government intervention as well as evaluate the potential impact and sustainability of proposed policies or investments.

Four Key Factors with Which to Assess the Microelectronics Ecosystem

Resilience

Microprocessor shortages for applications ranging from gaming consoles to automobiles and medical devices highlight the

challenges to resilience posed by microelectronics production specialization and concentration.⁴¹ Today, TSMC and Samsung build all high-density microprocessors having less than 7 nm features, which power the most highly sophisticated computing devices.⁴² Intel is working to regain parity, while a larger number of companies build the less-advanced semiconductors with larger node sizes used in other consumer electronics, military systems, and critical infrastructure. Because their profits are lower compared to high-end semiconductors, fabrication capacity of larger node size chips such as those used in automobiles has evolved to meet demand and switching the type of IC a given facility produces can take months to complete.⁴³ Consequently, a combination of facility fires in Japan and ice storms in Texas recently disrupted vehicle IC supplies for almost a year.⁴⁴

Besides foundries, a small number of providers have a dominant share of the market in other major steps in the microelectronics-

production process such as ATP. Of the steps comprising the semiconductor production process, only design and IC integration into equipment have significant supplier diversity.

Geopolitical disruptions also pose a threat to microelectronics resilience. The concentration of chip fabrication, packaging, and testing performed in Taiwan creates a risk of severe disruption or complete interdiction of supplies should that country's government come under pressure from the neighboring PRC regime, which depends on Taiwan for semiconductors. Although a PRC invasion of Taiwan is unlikely and mainland China is Taiwan's largest trading partner overall, the PRC government regularly interferes with Taiwan's computer networks and electromagnetic spectrum. It also possesses the air and naval capabilities to block Taiwan's access to raw material imports and semiconductor customers should it decide to do so.⁴⁵ The threat of military action coupled with economic coercion and information warfare could prove sufficient to convince Taiwan to limit its companies' participation in the global microelectronics ecosystem, although the economic consequences for Taiwan could be severe.

National security applications, which comprise about 10 percent of overall US semiconductor demand, arguably constitute the area of greatest concern with respect to microelectronics ecosystem resilience. The DoD initiated a trusted foundry program in 2003 to ensure secure production of chips for use in defense systems, but trusted foundries currently provide only about 2 percent of DoD ICs.⁴⁶ US national security applications therefore remain dependent on the relatively concentrated IC production base, especially in Taiwan.

To be effective, policies intended to increase microelectronics resilience should consider concentration in each step of the production process and across all IC categories. For example, blanket proposals to fund foundries in general ignore the fact that some chip types have much more greatly concentrated fabrication segments than others. And beyond fabrication, US

government investment could achieve greater impact per cost by establishing domestic ATP providers, which are currently concentrated in Taiwan, Japan, Korea, and Malaysia.

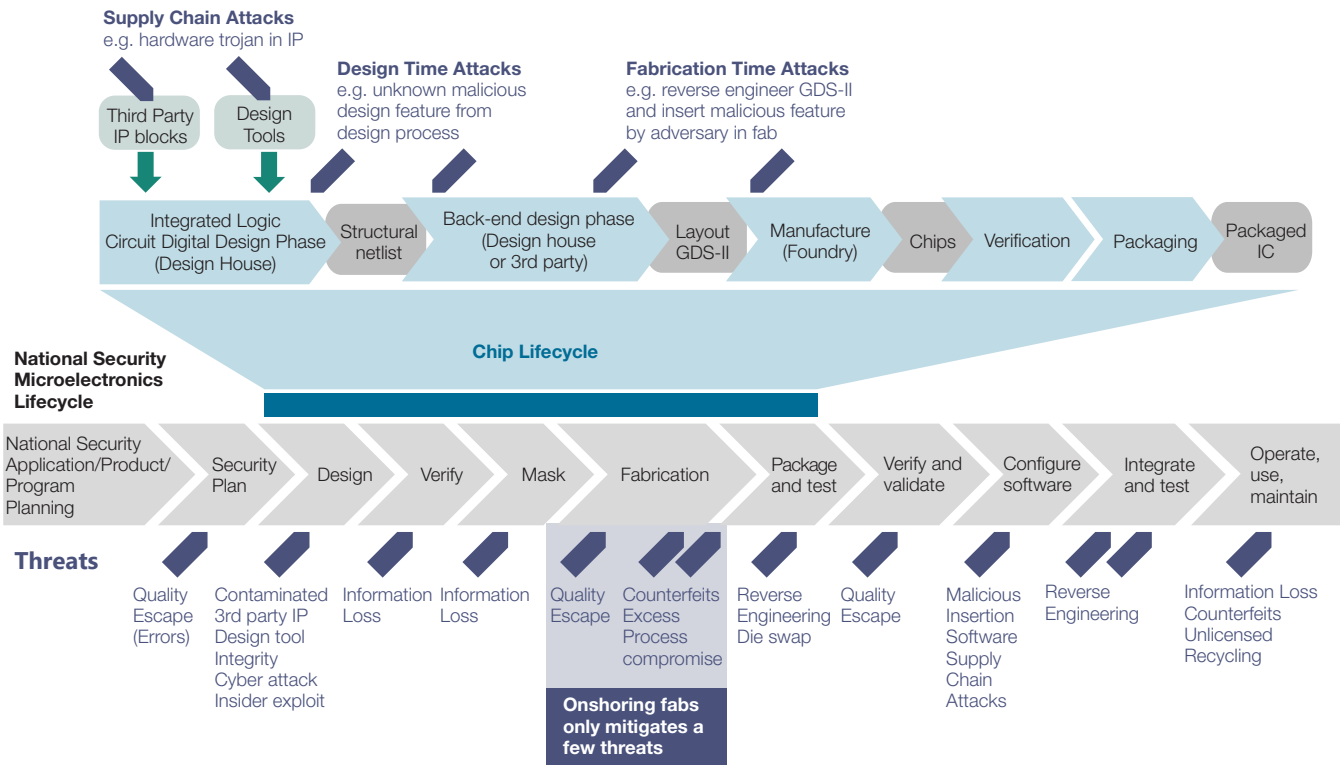
Assurance

Security vulnerabilities can be introduced at all stages of the microelectronics supply chain, as shown in Figure 6, but *verification testing*, which verifies that an IC has been built according to its design, and *validation testing*, which determines whether or not a circuit performs as it was intended to, can reveal many such liabilities. In the context of this study, *assurance* is defined as the ability to detect security vulnerabilities through hardware *verification and validation (V&V) testing*⁴⁷ or by other advanced design and architectural features that stymie malicious actors.

Microelectronics vulnerabilities can be classified into three primary categories: flaws, bugs, and back doors. Component manufacturers and service providers can unintentionally incorporate *bugs*, which are due to inconsistency between chip design and as-built configuration, or *flaws*, in which faulty design causes an IC to either fail or be unable to perform its intended function. In contrast, *back doors* are deliberately and illicitly incorporated into hardware by semiconductor suppliers, packagers, software companies, or other bad actors and can then later be activated to disable, slow, disrupt, or clear the system's memory at a predefined moment in time or can activate a hidden circuit in response to an external signal. Back doors can also be used to introduce hidden features into a system, such as circuits that exfiltrate data using an electromagnetic emission or stray signal that the exploiting party is prepared to receive.⁴⁸

Although bugs, flaws, and back doors pose significant security challenges no matter where they emerge, their presence is most consequential in national security microelectronics applications such as DOD weapons systems and critical power, communications, and transportation infrastructure.⁴⁹ US peer competitors such as the PRC and Russia would in all likelihood invest substantial effort and funding into developing

Figure 6: Security vulnerabilities in the microelectronics lifecycle



Source: Authors

back doors capable of avoiding detection through V&V. DoD's trusted foundry program was intended to address the threat of intentionally introduced microelectronics vulnerabilities, but only supplies a small percentage of DoD's total IC demand. Moreover, the complexity of modern microelectronics is such that even an IC that has been domestically fabricated, validated to have no known vulnerabilities, and verified as having been properly manufactured, unanticipated security flaws can still be discovered subsequent to the system being fielded. This occurred in 2021 when attack opportunities in the Micro-Op Cache of some Intel ICs was discovered.⁵⁰

Opportunities to insert intentional vulnerabilities will likely increase as computer programs known as *firmware* play an

increasingly important role in hardware operation. FPGAs already use firmware to program their gate or transistor configuration, and SoC designs require firmware to manage information flows between different chiplets or layers of complex ICs. Although programmed into a chip and not intended to be easily changed following production, firmware instructions could be written so as to provide still another access point through which to interfere with an IC's operation or exfiltrate data.⁵¹ Conversely, firmware also presents an opportunity to mitigate upstream vulnerabilities by modifying system behavior in ways unanticipated by a malicious actor.

Rather than increasing assurance solely through creation of trusted ICs, more promising approaches to future

microelectronics security are technological in nature. In these approaches, users would view individual ICs as *untrusted*, but could view as *trusted* the overall circuit or SoC in which individual ICs are integrated.⁵² DoD is currently pursuing a zero-trust model for microelectronics assurance in which improved design features and testing approaches prevent or detect vulnerabilities or—should they be present but not be detected or eliminated—minimize the harm they can cause. Included in these efforts are disaggregated SoC designs using heterogeneous components, including chiplets, in which the final circuit configuration is unknown to fabrication and ATP providers, thereby reducing the ability of adversaries to introduce effective back doors.⁵³

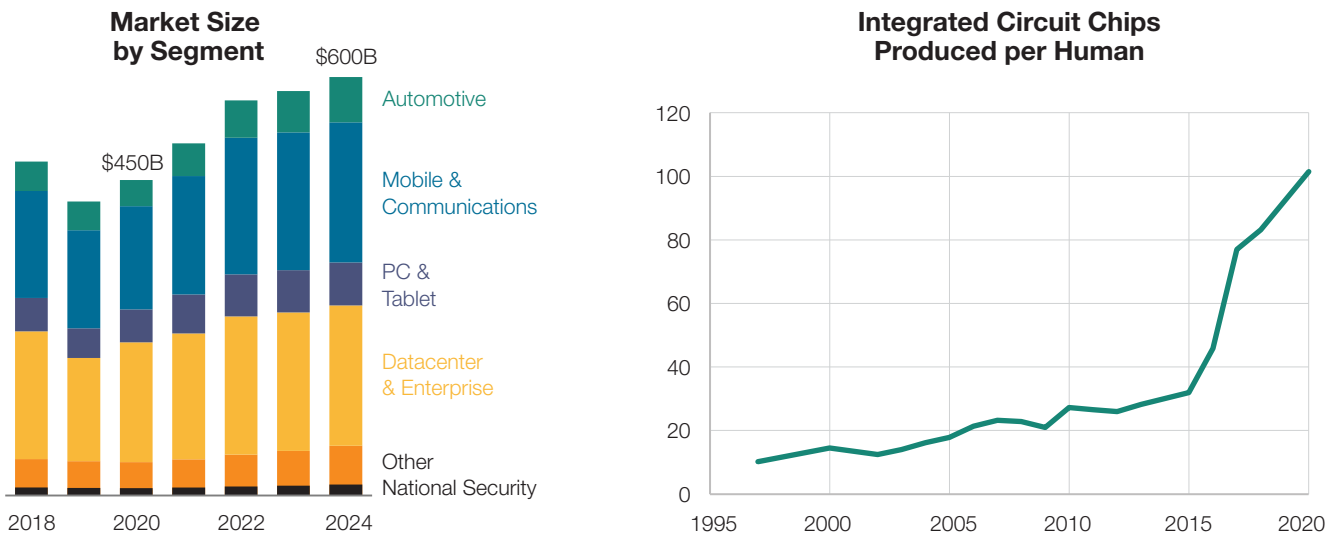
As noted in Chapter 1, onshoring fabrication facilities within the United States will not by itself achieve microelectronics

assurance. Vulnerabilities could be introduced in design or production steps other than fabrication, and US foundries would not be immune to the introduction of bugs, flaws, or back doors into ICs. However, greater diversity of fabrication and ATP facilities would, at some cost in time and money, offer customers alternative suppliers when security concerns arise at an existing provider. Over the long term, developing and adopting new approaches to obtain trusted microelectronics from untrusted sources will constitute a more effective and robust approach to achieving security compared to increasing domestic IC production.

Demand

The microelectronics ecosystem’s configuration has always reflected the needs of contemporary use cases. For example, customers’ pursuit of lower prices and improved performance

Figure 7: Microelectronics market growth



The overall microelectronics market is growing, led by increases in automotive and data center & enterprise demand.

Figure Source: Authors, Data Source: SIA and original research by the authors.

incentivized supply chain disaggregation and the concentration of most supply chain steps among a small number of performers. Across all IC applications, vehicle controllers, data center microprocessors and memory, telecommunications modems and processors are experiencing the highest growth rates.⁵⁴ The ecosystem has therefore evolved to include around a dozen makers of chips like those used in automobiles and data centers; more foundries would likely build high-end microprocessors but are unable to do so by the challenges associated with small-node semiconductor manufacturing.⁵⁵

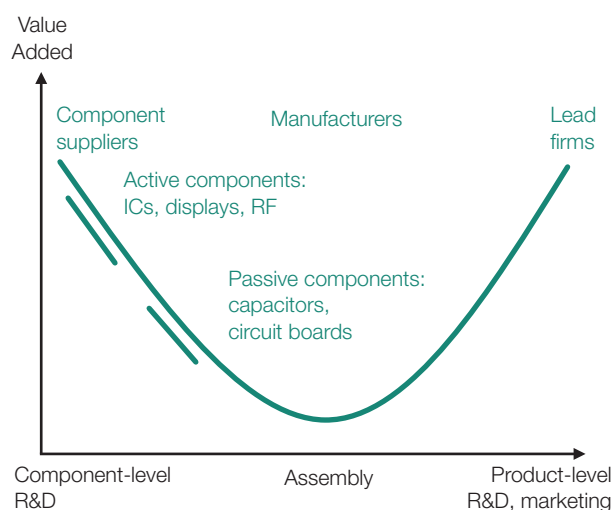
As shown in Figure 7, the microelectronics industry currently produces more than 100 chips per year per human, and the industry's products include an expanding range of designs and sophistication—triple the output of five years ago and with no signs of slowing. Given the dynamism of IC demand and the reactive nature of manufacturing, expecting supply-side policies to effectively shape microelectronics ecosystem structure is naïve.

Demand should therefore be a significant consideration in the development of policy and funding proposals designed to improve the US microelectronics ecosystem. Government initiatives that do not support customer expectations with respect to price, performance characteristics, and availability are unlikely to penetrate the ecosystem and achieve their intended goals of increased ecosystem resilience, assurance, or competitiveness. Moreover, policy and investment interventions that fail to satisfy current demand will be unsustainable without continuing government support.

Value Added

In addition to current demand, the microelectronics supply chain is shaped by the profit associated with differing IC types and the value added by various production steps. For example, although relatively small-node CPUs and GPUs boast higher profit margins than do other ICs, the fabrication plants that build small-node types require the greatest up-front capital investment and require frequent equipment and

Figure 8: The “smiling curve” of value-added in electronics production



Source: Namchul Shin, Kenneth L. Kraemer, and Jason Dedrick, “Value Capture in the Global Electronics Industry: Empirical Evidence for the “Smiling Curve” Concept,” *Industry and Innovation*, Vol. 19, No. 2, 89–107, February 2012. <http://dx.doi.org/10.1080/13662716.2012.650883>

facility upgrades to keep pace with the latest advances. In contrast, less sophisticated, large-node ICs garner lower profits but entail relatively smaller up-front costs and are often made at existing fabrication plants that no longer build leading-edge semiconductors. These contrasts in size of initial outlay and upgrade requirements, coupled with ample demand, incentivize a large number of manufacturers to produce older-design memory, control, and timing ICs whereas only the two incumbents currently build high-performance, small-node ICs with node sizes of less than 7 nm.

The number and diversity of microelectronics equipment and service providers are also influenced by the contribution of their efforts to the overall price or performance of final products, with those delivering the most impact contributing the highest value added. Consequently, the microelectronics supply chain can also be characterized as a *value chain*. Production steps

Figure 9: US market share of the semiconductor value chain

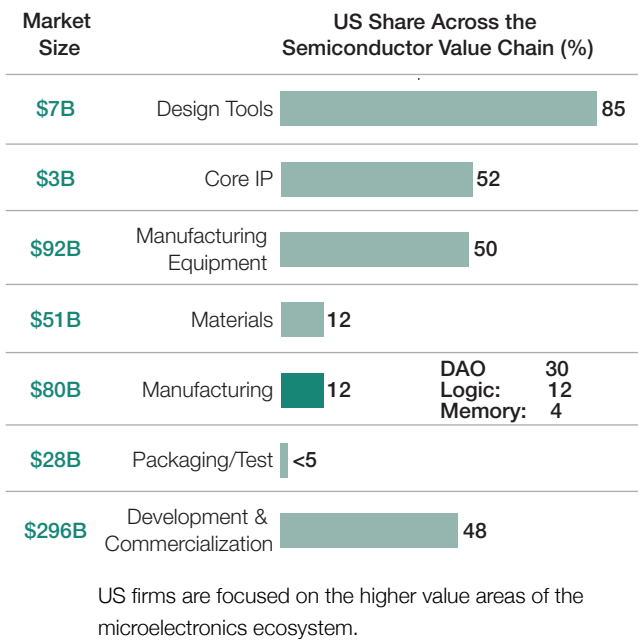


Figure Source: Authors, Data Source: BCG Analysis, Original Research, SIA Data

that add greater value are often more profitable, but also offer greater challenges to effectively implement because of the relatively higher investment or greater technical proficiency they require.⁵⁶ As argued by Namchul Shin and demonstrated by subsequent research (see Figure 8), the greatest value-add occurs on the two ends of the production process: on one end, component-level research and development (R&D) and manufacture of sophisticated components needed for the product, e.g., small-node microprocessors, and, on the other end, R&D, marketing, and branding of the overall product, such as an iPhone. Assembling components into products and producing such commodity ICs as controllers or timing chips fall in the middle and offer the lowest value added.⁵⁷

Structural currency disadvantages and high labor prices in the United States incentivize US manufacturers to focus on those

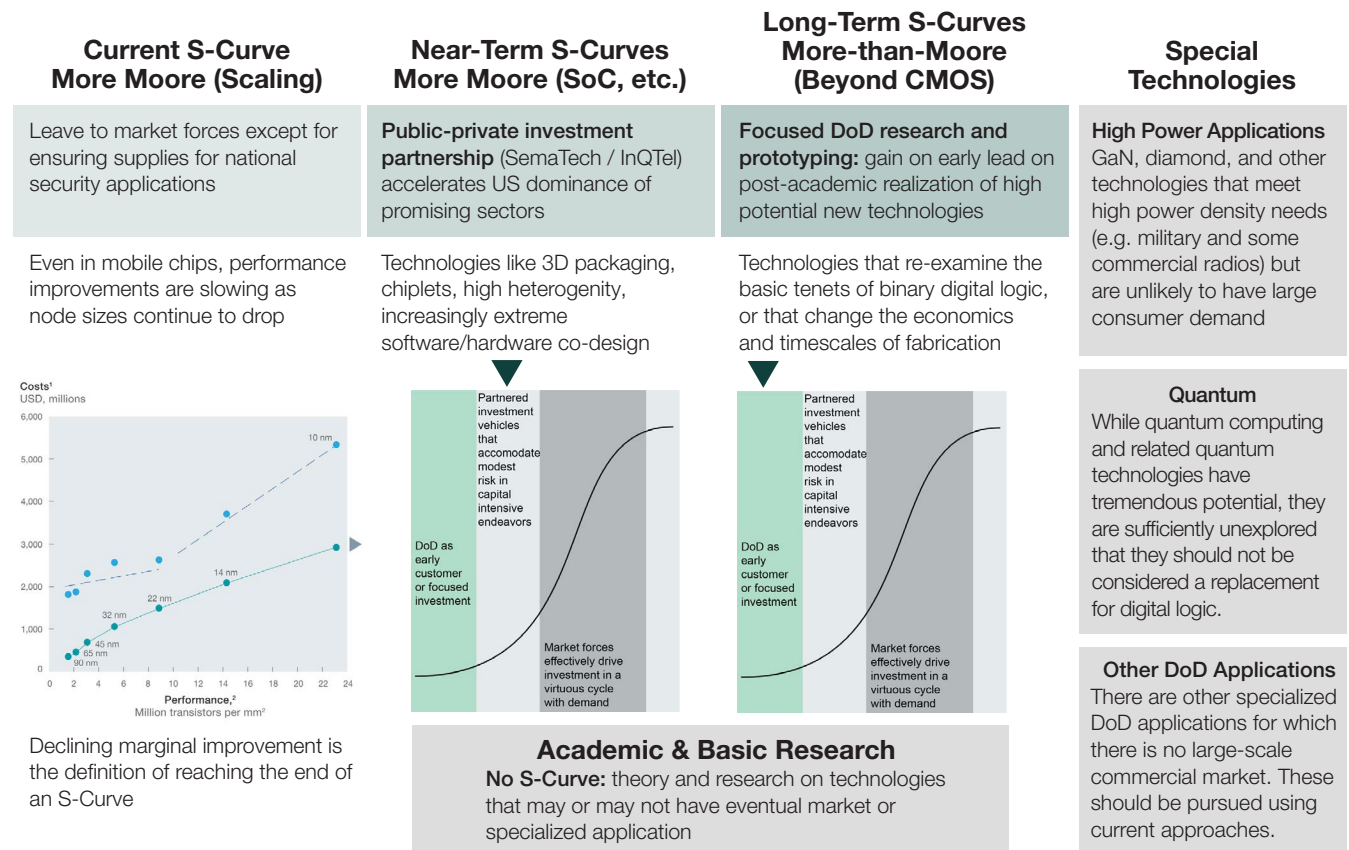
portions of the production process which have the highest value added and can therefore command premium prices (see Figure 9). In contrast, the focus of relatively new entrants into the industry based in Taiwan, the PRC, and South Korea is still predominantly component production and assembly, which, although essential, offer lower value and profits. Asian firms currently attempting to move up the value chain to new disaggregated or SoC and SiP architectures are hindered by the need to obtain scarce design talent and US-built EDA tools and manufacturing equipment, as well as the “innovator’s dilemma,” or the need to devote resources and capability to shrinking nodes sizes in their current designs instead of retooling to introduce next-generation technologies.⁵⁸

In addition to shaping the current microelectronics ecosystem, the value added by different production segments reflects their ability to address future demands. High value-added products and services—e.g., improved design tools, new classes of manufacturing equipment, and innovative core IP capable of increasing diversity in computing architectures—will be central to developing and fielding new ICs that provide increased levels of performance and security through small node size, disaggregated designs, and increased heterogeneity. The rising importance of complex architectures will also increase the value added associated with ATP, making it a potentially attractive area for US government investment.⁵⁹

Moving Up the Value Chain

The microelectronics ecosystem encompasses production elements characterized by their relative degrees of resilience and assurance; customers wanting microelectronics to use in current applications; and prospective customers seeking ICs with improved performance and security for existing or new use cases. As shaped by a relatively free market, today’s ecosystem effectively aligns supply with demand and responds to evolving customer expectations or exogenous shocks such as the COVID-19 pandemic. The fact the ecosystem works, however, does not mean it

Figure 10: S-curve growth models reflecting different technologies in the microelectronics supply ecosystem



The microelectronics supply ecosystem encompasses current, near-term, and long-term technologies that develop along “S-curves” characterizing their development.

Source: Authors

is problem-free, as evidenced by the existing and potential resilience and assurance shortfalls described in Chapter 2. Government intervention may be needed to address these concerns and help the US microelectronics industry remain competitive as rivals in China, Taiwan, and South Korea move up the value chain into design, component R&D, and product development.

In pursuing resilience, assurance, and competitiveness, government efforts should be sustainable and target areas that offer the most leverage. For example, although the US government could fund construction of additional US fabrication and ATP capacity for current-generation chips, overseas competitors such as national champions TSMC and Samsung would still retain advantages based on their proficiency, existing

customer base, lower labor costs, and pervasive government financial and regulatory support. Consequently, prices for US-built ICs would most likely be higher than comparable ones built abroad, and ongoing federal support would be needed to keep US fabrication facilities in business.⁶⁰ US government funding could be used to close the cost differential between US and overseas fabrication or ATP, which would make the business case for US production facilities more attractive and enable US firms to obtain corporate or other private funding for expansion or new construction.

Supporting ongoing fabrication or ATP operations would require less funding compared to construction and equipment and could enable more US government investment toward R&D of new semiconductor technologies in which US chip companies can establish an advantage, similar to the initial development of ICs during the mid-20th Century. Government resources will be essential to future microelectronics competitiveness, considering the multi-billion-dollar annual R&D investments being made by foreign competitors such as TSMC.⁶¹

Typically, the US government funds basic research into potentially useful new technologies and provides episodic, project-based funding for applied research into promising advances that emerge from basic research. The US microelectronics industry also invests in R&D, but its aim is usually evolutionary improvements on existing commercial technologies that are already fielded. As shown in Figure 10, today's mature IC technologies, which achieve incremental performance improvements or security gains over time, occupy the upper flat portion of their developmental "S-curves." These sustaining technologies typically follow Moore's law and increase performance through industry-sponsored R&D, which enables them to increase scaling and achieve greater transistor density.

However, little of either US government or corporate investment is typically directed at closing the gap between applied research and commercially viable products. This is a problem experienced

particularly by DoD and is characterized as the "valley of death" for new defense technologies. Within the microelectronics ecosystem, this gap occurs because government sponsors are unfamiliar with semiconductor market dynamics and do not know what technologies could be commercially viable or how to best market them; manufacturers are frequently unable to justify to their shareholders long-term investments in unproven technologies; and venture capital firms are reticent to invest in the microelectronics industry because of its high capital intensity and distant returns on investment.

Future technologies offer more leverage for government investment than do current technologies because they exploit the United States' position as a leader in high value-added component and product design, production of manufacturing equipment, and marketing and distribution. With respect to near-term future IC technologies occupying the steep portions of their S-curves and just entering the market, US microelectronics firms could, through government-sponsored applied research, expand beyond their existing strengths at the ends of the smiling curve of Chapter 3 and diversify into ATP, which will be critical to new disaggregated architectures such as SoC, SiP, and 2.5 or 3D chips. These efforts would build on government incentives provided to increase fabrication in the United States. Near-term future technologies also offer relatively certain and proximate returns on investment, making them more attractive to private capital. A *public-private partnership* (PPP), like those employed by In-Q-Tel and SemaTech, could fill the gap for these technologies between applied research and commercialization. Government co-investment in the partnership would catalyze the deployment of private capital while also benefiting from insights of private investors regarding market and demand trends.⁶²

Future technologies just beginning to move up the S-curve are unlikely to attract private capital to the same degree as more mature near-term advances, because their returns are rightly viewed as less certain and more distant. Long-

term microelectronic technologies are generally pursuing performance characteristics that exceed those governed by Moore's law for CMOS-based semiconductors and include such approaches as *mixed-signal* chips which combine analog and digital ICs, complex 3D SoCs, and non-CMOS semiconductors and architectures designed for high-power applications or quantum computing. Government-sponsored basic and applied research will therefore be required to develop long-term IC technologies.⁶³

When they have matured and moved farther up their S-curves, long-term technologies could transition into commercial use via a PPP, such as in the evolution of GaN semiconductors from military radars to 5G radios.⁶⁴ Other new technologies could have primarily military or government applications and

only modest commercial ones and may depend on continued government funding.

The proposed framework of resilience, assurance, demand, and value added provides a more holistic way to assess the microelectronics ecosystem than simply identifying chokepoints and bottlenecks in today's supply chain. Since the objective of employing a supply chain model is to guide actions intended to improve the chain's functioning, incorporating future as well as current customers is essential to estimate the likelihood of potential initiatives being effective and enduring. In the next chapter, the proposed framework will be applied to existing and potential future proposals currently under consideration for US government intervention into the microelectronics ecosystem.



CHAPTER 4. APPLYING THE FRAMEWORK

The microelectronics industry has long argued that the US government should grow domestic fabrication capacity in order to counter the East Asian concentration of foundries and improve IC resilience and assurance for national security applications.⁶⁵ Although fabrication is the most visible and capital-intensive part of microelectronics production, it is not the only chokepoint with the potential to affect IC supply resilience, and US government funding may achieve a greater impact by advancing the introduction of new chip technologies where the US microelectronics industry can establish an advantage. The 2021 NDAA's CHIPS Act and DARPA's Electronics Resurgence Initiative recognize the need for a more holistic approach to government intervention by including options to develop new technologies alongside funding new fabrication and ATP facilities.⁶⁶

The four-factor framework proposed in this study enables a systematic way to identify production segments for which federal policy or funding might be warranted and beneficial. Because the framework is intended to guide US government interventions, the potential impact of each segment on IC resilience, assurance, demand, and value added is evaluated from a US perspective. To represent US customers, resilience and assurance are measured in terms of ICs supplied to the US market from the global supply chain; to represent US manufacturers, demand reflects the ability of US companies to address contemporary market needs; and value added assesses the US microelectronics industry's ability to add value via that production segment.

Photo caption: A scientist examines an electronic display depicting a silicon wafer. (Monty Rakusen/Getty Images)

Figure 11 summarizes application of the four-factor framework to the current microelectronics ecosystem based on recent assessments by a range of industry, academic, government, and trade organizations, including the Semiconductor Industry Association, International Electrical and Electronics Engineers (IEEE), Congressional Research Service, and National Cyberspace Solarium Commission.⁶⁷ This assessment is subjective, of course, and other analysts may interpret the state of the microelectronics ecosystem differently. This study's main argument is that a comprehensive framework such as the one depicted in Figure 11 is needed to provide a starting point for formulating government policy and investment in the IC area. Each segment's assessment is briefly described below.

Assessing the Microelectronics Ecosystem from the US Perspective

Fabrication

The concentration of fabrication capacity into a relatively small number of facilities reduces the fabrication segment's resilience, and exacerbating this reduction is the geographic clustering of capacity for some IC types, such as <7 nm node size GPUs and CPUs, which are only produced in Taiwan and South Korea. Because testing can often detect backdoors, this level of concentration need not reduce assurance, but the lack of fabrication diversity reduces options when a customer is dissatisfied with a foundry's efforts to eliminate such vulnerabilities. Sometimes testing can detect flaws and bugs, but V&V is often only able to catch known phenomena and is an incomplete solution for assurance.

The focus of US fabrication facilities, which supply about 12 percent of today's demand, is legacy chip types that can be profitable despite the US's relatively high-cost structure. US fabrication firms could gain an advantage if they were to lead in the introduction of new technologies such as SoC or 3D and heterogeneous ICs that incumbent fabs overseas may be less well-positioned to adopt due to their need to support

current customers with sustaining advancements along today's S-curve. However, new chip architectures depend on leading-edge fabrication capabilities that are only present at small scales in the United States, which will require some improvement in high-end US-based fabrication capacity.

Packaging






























The ATP segment of semiconductor production separates etched silicon wafers into chips and prepares them for installation in customer systems by incorporating connectors and mounting hardware or in some cases combining ICs into higher assemblies such as SoCs or SiPs. Although generally not as concentrated as fabrication, packaging for the most sophisticated chips is becoming increasingly limited to a few firms with the requisite equipment and skill. The geographic clustering of ATP firms in East Asia reduces resilience but impacts assurance less severely since packaging offers few opportunities for exploitation.

Expanding packaging to the United States would be challenging due to relatively higher labor and regulatory costs. However, US microelectronics manufacturers moving up the value chain to SoC, 3D, and heterogeneous chips could also entail an opportunity to enter the packaging market because of these ICs' higher price point and need for new packaging technology. An increase in US ATP firms could also directly benefit the DoD by creating highly customized and secure SoC or SiP ICs constructed using less-sophisticated ICs, thus allowing the DoD to gain the benefits of customized near-leading-edge capability without also bearing the full burden of the concomitant investment.

Design

Although the most sophisticated ICs are fabricated overseas, more than half are based on US designs, helping US firms meet current demand and lending resilience to the US market. Flaws, bugs, or back doors introduced during design could be difficult to detect through V&V testing, but US-developed

Figure 11: The framework can assess the impact of each production segment on US microelectronics supply resilience and assurance, and the ability of the US microelectronics industry to contribute to current and future demand.

SEGMENT	 INCREASING IMPACT			
	 RESILIENCE TO US CUSTOMERS/USERS	 ASSURANCE TO US CUSTOMERS/USERS	 US ALIGNMENT WITH TODAY'S DEMAND	 US ABILITY TO ADD VALUE
Fabrication	 Small-node foundries concentrated in East Asia	 Many backdoors can be detected by US V&V	 US fabs competitive in narrow areas of market	 New designs could command premium price
Packaging	 Most, but not all, ATP and OSAT firms in East Asia	 Minimal undetectable backdoor opportunities	 US not competitive due to labor and regulatory costs	 US ATP for SoC, 3D, etc. could warrant higher cost
Design (Core IP)	 US leads in number/sophistication	 Vulnerabilities can be hidden, but most IP is US	 Strong demand for current, emerging US designs	 US could exploit lead in core IP for new designs
Design tools	 US supplies essentially all design tools	 Malware could enable back doors; but tools are US	 US design tools used throughout industry	 US tools remain essential for exploiting new tech
Manufacturing Equipment	 US or allies supply nearly all high-end equipment	 Undetectable vulnerabilities unlikely	 US and European equipment predominant	 Break from smaller nodes could grow US value add
Validation and verification	 Largely done overseas, but oversight is strong	 Poor V&V could miss bugs, etc., but is US-based	 US does not provide substantial portion	 New designs could justify higher US costs

The framework can assess the impact of each production segment on US microelectronics supply resilience and assurance, and the ability of the US microelectronics industry to contribute to current and future demand.

Source: Authors

core intellectual property could reduce the likelihood of such potential vulnerabilities being introduced into products intended for US customers. US leadership of their designs would also position US firms to be able to contribute to long-term future technologies, which would derive much of their value from core IP. As computing architectures increase in heterogeneity and move away from x86, PowerPC, and other standardized models, opportunities are growing for novel designs and for IP specialized to support certain forms of processing, like signal processing that can benefit more from software-hardware co-design than decreasing node size.

Design Tools

Similar to IC designs and core IP, the dominant market position of US-developed EDA tools increases the resilience and assurance of the microelectronics supply chain for US customers. They also play an essential role in the design of more than 80 percent of the chips sold to satisfy current demand, and they will play a central role in adding value to future chip technologies. As technologies like 3D packaging and increasingly heterogeneous SoCs mature, new design tools will be needed, providing a unique opportunity to expand the US lead in this area.

Manufacturing Equipment

US-built equipment manufactures half of the ICs produced today, fostering ecosystem resilience and supporting current customer requirements. Because undetectable flaws, bugs, and back doors are unlikely to be introduced through manufacturing equipment, the prevalence of US-made manufacturing equipment does not substantially improve assurance. In addition, US companies do not build the EUV equipment needed to continue shrinking node size and so increasing IC density along the current S-curve. However, US equipment suppliers could exploit their strong overall market position to more easily implement new near-term and long-term future IC designs that do not rely solely on shrinking node size to advance technologically.

Validation and Verification

ATP firms test ICs as part of the assembly and packaging process but may not fully validate that ICs are constructed as designed or verify that they will perform as intended under all realistic conditions. For this reason, V&V is usually the responsibility of the organization that receives the finished IC and that often also designed it. V&V and oversight of the IC manufacturing process by US-based customers or IDMs increases ecosystem resilience, but compromised or insufficient V&V could significantly degrade assurance. US firms do not contribute substantially to ATP, but their oversight and V&V capabilities could be leveraged to add value in future IC technologies, supported by the DoD's efforts to develop zero-trust models of microelectronics integration.⁶⁸




































Evaluating Potential Solutions

The assessment framework described above suggests opportunities for US government policies and investment to improve the resilience, assurance, and competitiveness of US microelectronics. For example, the current lack of diversity in fabrication undermines resilience and assurance, but US foundries may not be competitive building today's leading-edge chips unless they receive financial support and leverage foreign expertise. This approach may be a bridge to future domestic fabrication facilities that could command higher prices by exploiting US strengths in core IP, EDA tools, and manufacturing equipment to move up the value chain and produce near- and long-term microelectronics technologies. This and other initiatives currently being considered are summarized in Figure 12 and assessed in the following paragraphs.

Support Operations of US Leading-Edge Node Fabrication and ATP facilities

Diversifying fabrication would improve microelectronics resilience and offer alternatives when an incumbent supplier's assurance is in doubt. However, US fabrication plants would likely not be cost-competitive in producing the most advanced chips against overseas facilities that have built competence in the newest manufacturing techniques, and which enjoy

Figure 12: Impact assessment of supply chain-strengthening proposals using the four-factor framework

INITIATIVE	COST	 INCREASING IMPACT OF INITIATIVE			
		 RESILIENCE TO US CUSTOMERS/USERS	 ASSURANCE TO US CUSTOMERS/USERS	 US ALIGNMENT WITH TODAY'S DEMAND	 US ABILITY TO ADD VALUE
Fund operation of US leading-edge node fabrication and ATP by US or US/foreign partnership	 \$1-5 Billion/year	 <5nm ICs could be replaced by new designs	 Modestly improved oversight in US	 Will meet some demand but lag leading edge	 US can leverage fab for design, core IP insights
Incentivize larger node fabrication in US or ally via tech transfer, purchase agreements	 \$5+ Billion	 Lower-end ICs more vulnerable to shocks	 Modestly improved oversight in US/ally	 Will meet demand at risk of overcapacity	 US can leverage fab for design, core IP insights
Stand up US public-private investment partnership for maturing near-term future tech	 \$5+ Billion	 New designs may be cost effective in US/Europe	 Near-term tech could offer greater security	 Maturing tech weakly aligned with demand	 US can exploit talent, design, IP, equipment
Accelerate "zero trust" and architectural approaches to provide assurance	 \$1 Billion	 US could perform more segments of value chain	 Could obviate many vulnerability concerns	 V&V rapidly growing; could be disrupted	 US exploit talent, design, IP, and customer base
Customer coalition with export/import/tariff guarantees	 \$<1 Billion	 Compel suppliers to diversify geographically	 Pressure on suppliers could improve oversight	 Could increase US competitiveness v. Asia	 Could build customer base for future tech
Fund research and prototyping of "new S-curve" technologies	 \$5+ Billion	 US could establish role in fab, ATP, V&V	 Heterogeneity can improve security	 Long-term tech weakly aligned with demand	 US exploit talent, design, IP, and customer base

Source: Authors

government subsidies, tax incentives, and lower labor costs relative to the United States.⁶⁹

US foundries and ATP facilities could produce leading-edge chips at a competitive price if they received government support to partially offset higher labor and compliance costs compared to overseas competitors. US-based Intel is attempting this course of action today.⁷⁰ Intel's initiative shows that corporate R&D funding is available to at least partially fund construction of new high-end semiconductor production capacity. The US government's support to leading-edge fabrication could therefore be less than private investment and center on tax or regulatory relief that would help foundries remain competitive once they are in operation. Ongoing support would also improve the business case for new US foundries, which will make them more attractive for corporate or other private capital that expects investments to begin paying off within about 5 years.

The US government could build on the establishment of domestic leading-edge fabrication capacity by devoting most of its microelectronics funding to sponsoring development of fabrication and advanced packaging capabilities for near- or long-term future chip architectures. These technologies depend on high-end fabrication capabilities and are not attractive for corporate R&D funding due to their distant return on investment. Government financing could catalyze the US microelectronics industry's movement up the value chain into new technologies where it could gain a greater market share of production segments outside existing US strengths in EDA tools, core IP, or manufacturing equipment.

Encourage Partnerships between US Fabrication, ATP Providers, and Foreign Industry Leaders

A significant limitation facing US chip manufacturers and ATP firms in establishing competitive leading-edge node IC production is the manufacturing expertise and customer relationships enjoyed by overseas rivals like TSMC and Samsung. Partnerships between foreign market leaders and US

IDMS such as Intel and foundries like Global Foundries could improve the competitiveness of US firms. This approach is not dissimilar from the offsets and technology sharing agreements often required by other national governments.⁷¹ In the US case, however, these voluntary partnerships could be incentivized by extending US government tax and regulatory incentives for ongoing operations, as described above for US firms, to foreign companies that participate.

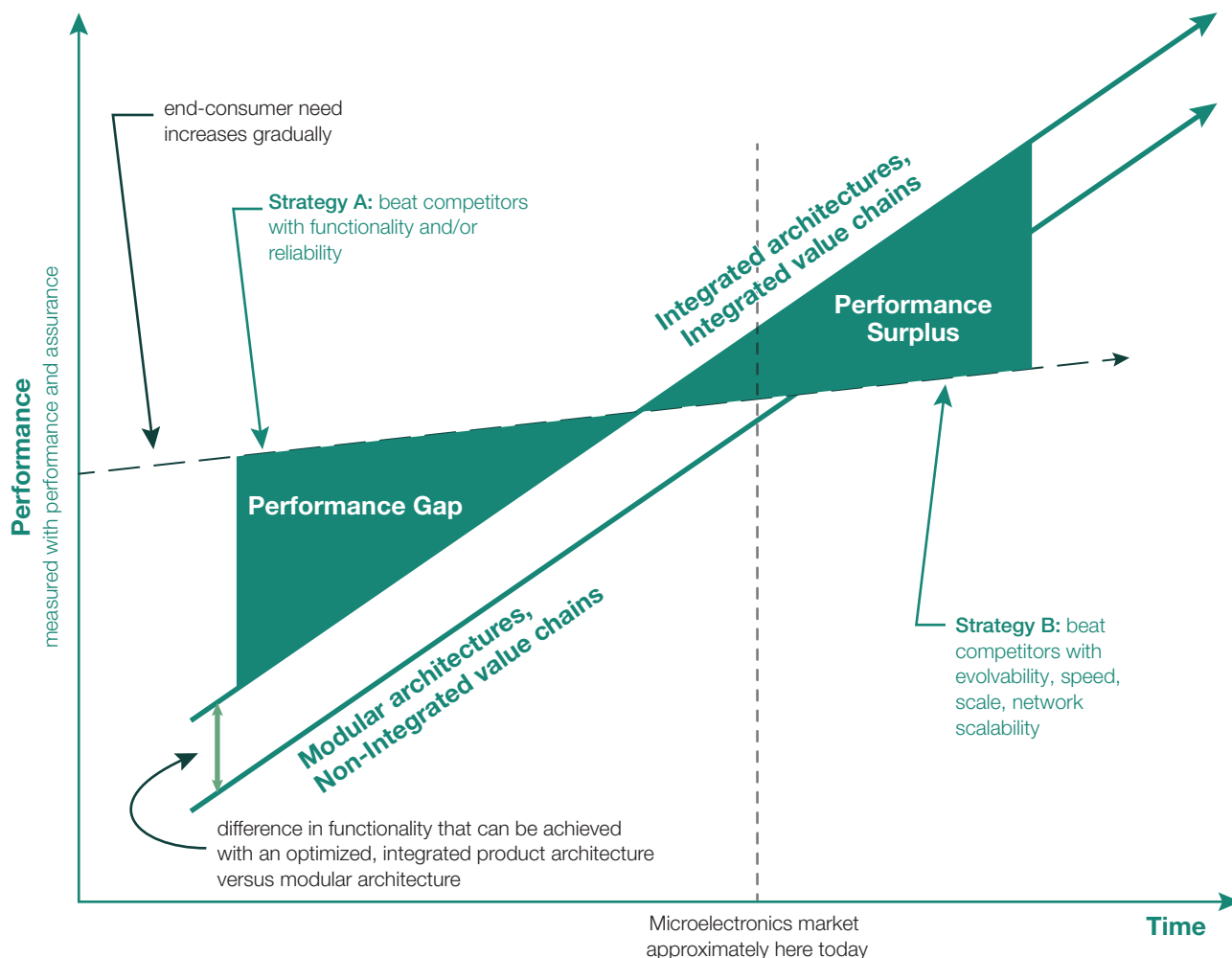
Incentivize Legacy Chip Fabrication and Packaging Among Allies

Current US foundries largely mitigate the impact of their higher cost structure relative to foreign rivals by manufacturing large-node microprocessors and memory chips using well-amortized infrastructure that previously built leading-edge chips. Some US fabrication plants also remain viable by tailoring ICs to customer needs in return for higher prices, such as in the trusted foundries that produce the 2 percent of DoD chips destined for the most critical national security systems.⁷²

One argument for expanding leading-edge chip fabrication and ATP in the United States is to support national security applications, but defense systems and critical infrastructure remain in service for decades and therefore almost exclusively rely on older-design, larger-node semiconductors. Paying premium prices to enable domestic fabrication of all chips needed for national security use cases would likely be unaffordable, as well as impractical due to the number of chips required. Moreover, complete domestic production of national security chips is unnecessary to improve assurance and resilience, which could be achieved through adequate diversification of fabrication or ATP capacity into the US as well as allied or partner countries.

As with the case of leading-edge node chips described above, new US fabrication and packaging facilities for larger-node chips will be less competitive than foreign rivals unless the US plants can exploit existing infrastructure or customer relationships. To level the playing field, the US government could incentivize

Figure 13: Value chain performance over time



Near-term future microelectronics technologies could disrupt the continued pursuit of small node sizes.

Source: Clayton Christensen and Michael Raynor, *The Innovator's Solution* (Cambridge, MA: Harvard Business Review Press, 2003).

domestic expansion of larger node capacity by committing funds to mitigate the cost differential created by overseas financial and regulatory support through tax incentives. In turn, the improved business case for US large-node foundries would help unlock private funding to construct fabrication and ATP capacity.

Although labor and regulatory costs in Europe may be similar to those in the United States, allied governments might be willing to invest in construction and operation of large-node or legacy foundries as a national priority. The US government could incentivize such allied investments with a combination of

technology-sharing arrangements with US firms and agreements to purchase allied nations' chip production for US defense or critical infrastructure applications. Additionally, partners such as India that currently have less advanced microelectronics industries could offer competitive cost structures compared to those of Taiwan and South Korea and might be willing to invest in IC production. And, although India would initially manufacture only less sophisticated chips, these ICs are and will remain necessary for most national security applications.

Form Public-Private Partnerships for Near-Term Future Technologies

A sustainable, long-term approach to improving US microelectronics resilience, assurance, and competitiveness would be to move up the value chain into new architectures that offer improved performance and reduced vulnerability beyond those on the current S-curve of shrinking node sizes. These approaches—including SoC, SiP, 3D and other disaggregated chip designs—employ new fabrication and packaging processes but would still rely on foundry capacity for the underlying ICs, which could be expanded in the United States and allies through other initiatives as described above.

More heterogeneous and disaggregated chip architectures offer the ability to create specialized characteristics that would justify the relatively high prices resulting from their unsubsidized manufacture in the United States or allied nations.⁷³ These technologies could also be viewed as a classic case of business disruption. By exploiting the ability to create a greater variety of customized solutions with greater assurance, disaggregated IC designs can better align to customers' needs and more easily adapt to new use cases. And as shrinking node sizes become harder and more expensive to achieve, near-term future architectures such as SoC or SiP could be less expensive and offer characteristics that are more attractive to customers than circuit density.

PPPs such as the National Semiconductor Technology Center established by the 2021 NDAA are useful mechanisms

through which to accelerate production of near-term future IC technologies that are already being fielded or are capable of delivery within 5 years. This model, like those used in the DoD's Manufacturing USA Institutes, combines federal funding and private capital to yield minimum-viable products and provide a return on investment within approximately a decade.⁷⁴

In the case of near-term future technologies, microelectronics PPPs would invest in those portions of the value chain where the US is capable of regaining its leadership, such as in fabrication or ATP, while leveraging existing US strengths such as core IP, EDA tools, and manufacturing equipment. By catalyzing greater diversity in the microelectronics ecosystem, PPPs could improve resilience, assurance, and competitiveness for US customers and industry. National security applications would eventually benefit from domestic production of ICs that incorporate new technologies but, due to switching costs, would likely wait to replace existing ICs until a future modernization cycle.

Accelerate Zero-Trust Technologies

Through improvements in V&V and the adoption of new disaggregated chip design and architectures, the DoD currently has several efforts underway to increase IC security for defense and critical infrastructure use cases. Some of these methods, for example those developed under DARPA's Security Integrated Through Hardware and firmware (SSITH) effort, foil malicious actors by randomly changing its microarchitecture every few milliseconds,⁷⁵ thus mitigating whole classes of vulnerabilities that can't be detected through V&V regardless of where a chip is manufactured. Although valuable for national security applications, the resulting zero-trust microelectronics also have commercial utility, the market for which will grow as concerns for cyber security continue to increase. As it did with GaN semiconductor technology during the 1990s, DoD could transfer some of these technologies to US companies pursuing near-term future IC architectures, such as those financed by PPPs as described above, to realize the value added created by this government investment.⁷⁶

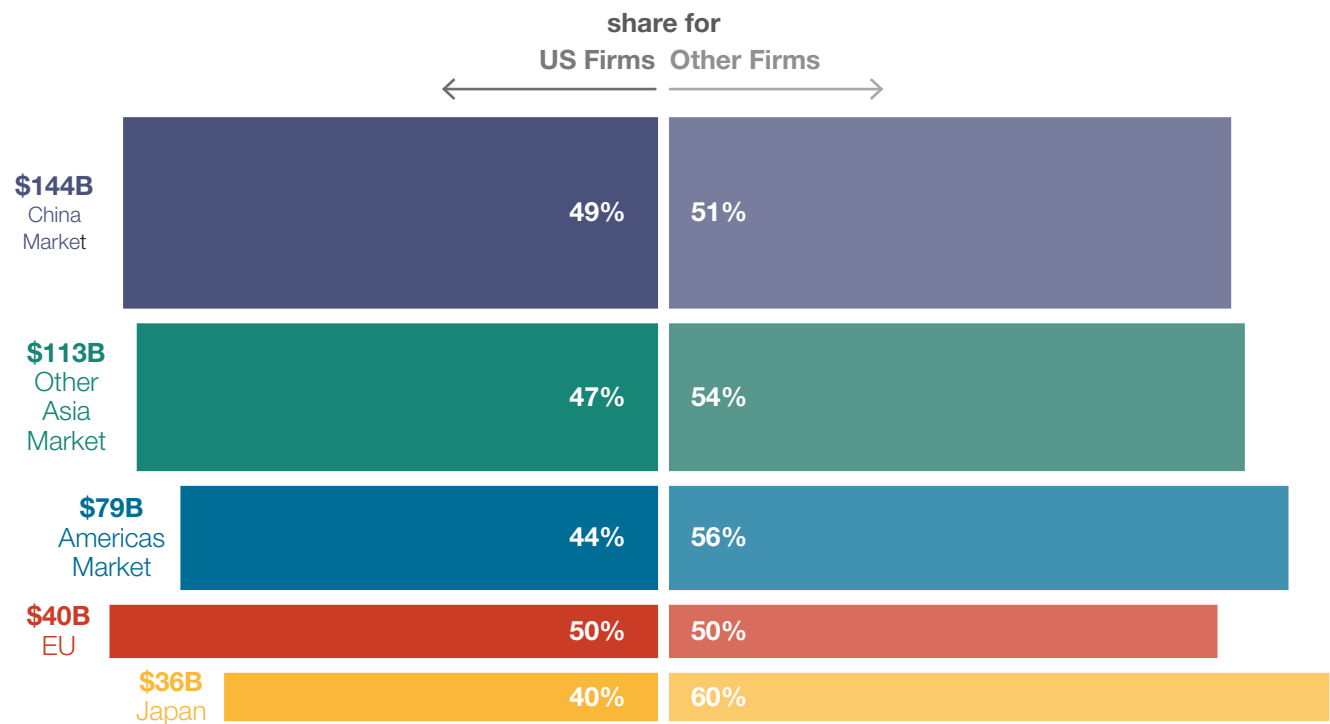
Establish a Customer Coalition

The concentration of producers in the microelectronics ecosystem gives them considerable market power while exposing their customers to substantial resilience risk and few options with which to address assurance shortfalls. This relationship is currently stable because the largest IC customers are in the PRC, the United States, South Korea, Japan, and Taiwan. With the exception of the PRC, these nations are also the world's largest IC producers (comprising 92% of IC market value) and are, moreover, highly dependent on one another because each specializes in a different segment of the microelectronics

value chain. As the largest single customer for chips, the PRC is capable of exerting some power over supplier countries, but as demonstrated by recent US export controls against Huawei, Beijing's influence is limited. The PRC government's influence will increase, however, as a larger number of PRC firms move into more segments of the IC production process, a trend that PRC leaders plan to accelerate as mandated by the Made in China 2025 initiative.⁷⁷

If the PRC becomes a dominant IC producer, Beijing would be capable of exerting more economic pressure on its neighbors

Figure 14: China's share of the global integrated circuit market



China is the world's largest and fastest growing customer for ICs, half of which are sold by US companies and more than three-quarters of which are fabricated and packaged in East Asia.

Source: SIA.com, June 2020, <https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf>.

than it currently can and with fewer concerns of provoking such backlashes as the export controls placed on Huawei. To mitigate the impact of the PRC's growing role in both microelectronics supply and demand and curb malign behavior by the PRC government, the US could assemble a coalition of major IC customer countries that would then be able to influence IC production by exerting their collective buying power. The coalition could, for example, coordinate export controls or tariffs they levy against the PRC to prevent damage to each other's industries and improve the effectiveness of trade actions against PRC efforts to undermine the goal of a free and open microelectronics market. This coalition could also cut off sales from TSMC in response to PRC attempts to control the company or Taiwan's government and thereby poison a key prize.

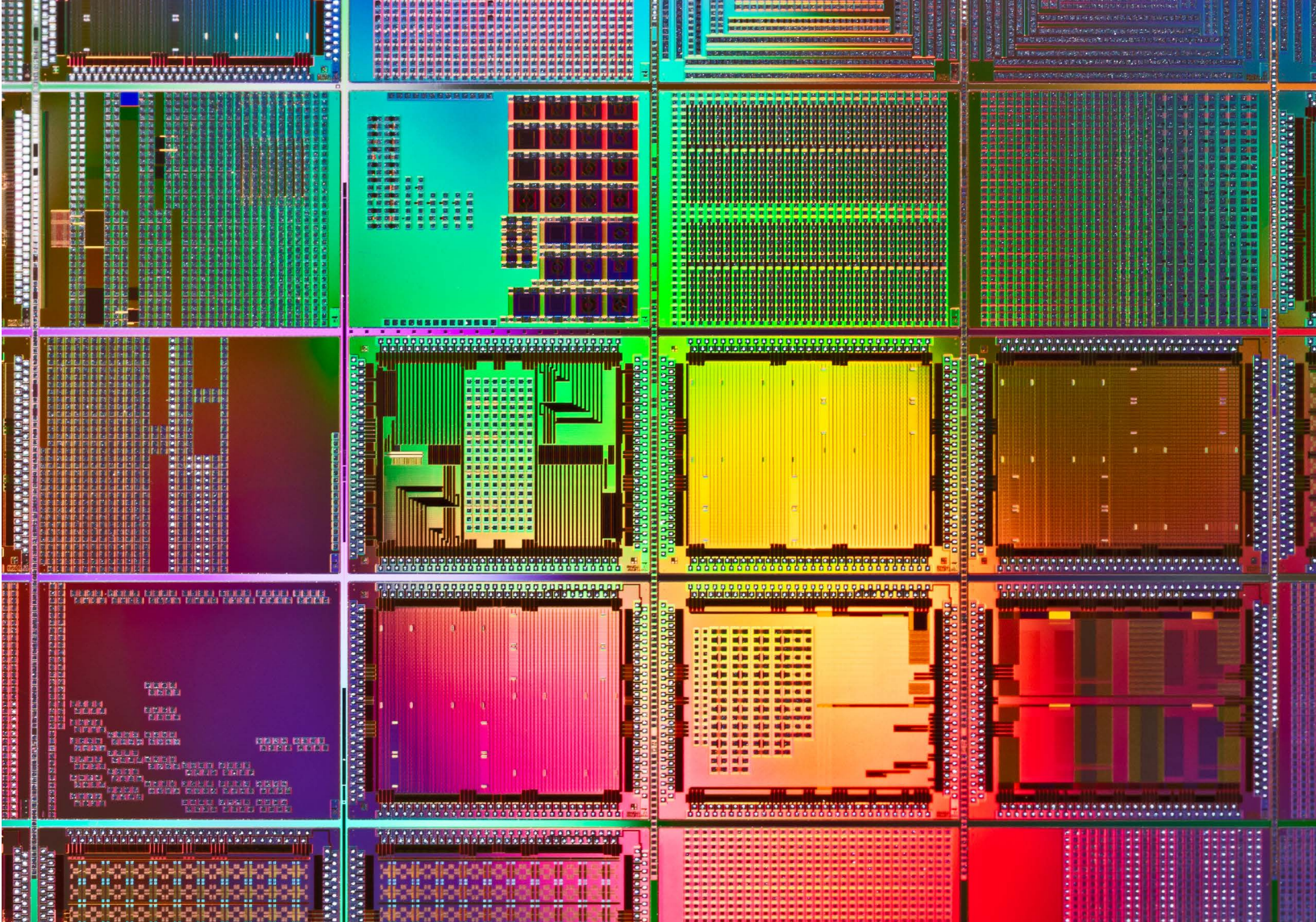
Fund R&D of Long-Term Future Technologies

The US government is already funding development of new IC designs that pursue new performance characteristics and logic architectures. Some of these long-term future technologies are

niche capabilities that may never achieve consumer use, like high-power systems using non-CMOS semiconductors such as GaN and diamond or hardware architectures for quantum computing. Other efforts might address long-term needs of the commercial market, such as moving beyond transistor-digital computing to create new architectural building blocks for data processing. Because of these technologies' distant maturation and uncertain applications, DoD research funding is appropriate during their early stages but something akin to a PPP would likely be required to transition long-term future technologies into commercially-viable products.⁷⁸

A Framework for Decision-Making

The above concepts are only a small selection of the possible approaches the US government could pursue to increase the resilience, assurance, and competitiveness of the US microelectronics industry and its customers. However, these examples show the utility that a comprehensive framework has in assessing the microelectronics ecosystem and the potential ways its challenges and opportunities could be addressed.



CHAPTER 5. A STRATEGY FOR INCREASING RESILIENCE, ASSURANCE, AND COMPETITIVENESS

Seventy years after their invention, microelectronics are now foundational to the US economy and essential to defense systems and critical infrastructure. Although the global microelectronics ecosystem has evolved to meet the demands of today's commercial and government customers, semiconductor resilience and assurance are increasingly at risk. The CHIPS Act and the American Foundries Act established mechanisms as part of the 2021 NDAA to begin addressing these challenges across the entire production process, from design and fabrication to packaging and testing, but have not as yet been funded.⁷⁹

Improving the dependability and security of US IC supplies will require greater diversity across the microelectronics value chain. However, new US-based production capacity is unlikely to be competitive with foreign manufacturers and service providers, which receive government financial and regulatory support and benefit from their countries' relatively low labor costs. To level the playing field, the US government authorized federal support in the CHIPs Act to build or expand domestic fabrication and

Photo caption: Photo: An extreme close-up of a multi-colored computer silicon wafer. (MirageC/Getty Images)

ATP capacity. The Congress is now considering appropriations for the CHIPS fund, which would allocate almost three-quarters of the funding toward building fabrication and ATP capacity for current generation chips.⁸⁰ This approach, however, does not address ongoing operational costs and fails to exploit the availability of corporate or other private funding for constructing and equipping production facilities.

This study proposes a different, two-pronged, strategy to achieve US microelectronics resilience, assurance, and competitiveness than that being pursued by Congress. The strategy's main line of effort and the bulk of government funding would invest in the US microelectronics industry's future to provide it an advantage over foreign competitors by exploiting the transition in chip design from simply increasing density to instead growing design complexity. Using government and privately funded research, US chipmakers could mature near-term disaggregated and heterogeneous architectures to move up the value chain and potentially get ahead of foreign competitors. This initiative, which would include manufacturing technologies and leverage US companies' current leads in core IP, EDA tools, and manufacturing equipment, would strengthen the US position in fabrication and ATP for new chip types. Further, by enabling the use of disaggregated architectures that obscure ICs' final configurations until final assembly by the customer, it would also improve assurance.

Government R&D investment would go beyond basic research and carry new microelectronics technologies through applied research to commercialization. Because creating a commercially-viable product depends on an understanding of markets and demand, new mechanisms such as PPPs would be used to guide government spending on near-term future IC technology development. The PPP can consider market demands and weigh the balance of investment between infrastructure and product in an agile fashion. Government sponsors would provide an investment base that reduces risk to private investors and shape investment decisions to reflect

government concerns and interests like security or operational utility.

Over the longer term, the strategy's main line of effort would provide government support to basic and applied research in next-generation technologies that would begin new S-curves, e.g., low-power digital IC designs,⁸¹ novel architectures,⁸² and new computing approaches with disruptive potential for future consumer markets. These efforts would complement existing DoD-sponsored basic and applied research into new technologies for use in national security applications, including ultra-high power analog ICs and new architectural paradigms like those applied in quantum computing. In combination, these R&D investment types would enable the US microelectronics industry to continue to move up the value chain by enabling them to sustain a first-mover advantage in fabrication and ATP and would offer additional opportunities to improve resilience through diversification.

Current proposals such as the United States Innovation and Competition Act of 2021 would allocate only about a quarter of its funding over the next five years, or about \$13 billion total, to R&D of near and long-term future IC technologies. For comparison, TSMC alone plans to spend \$6.3 billion on R&D during 2021.⁸³ To attempt to get ahead of foreign competitors and establish an advantage in new IC technologies, the US government should rebalance its funding priorities away from expanding capacity for current generation chip production and toward R&D in support of two initiatives described in Chapter 4:

- Form US public-private investment partnerships to mature architectures and manufacturing techniques for such new near-term technologies as SoC, SiC, 3D and other heterogeneous and disaggregated chip designs.
- Fund research and prototyping of long-term computing hardware technologies emerging from basic and academic research.

The strategy's second line of effort would address the current IC market by advancing four of the initiatives described in Chapter 4. These programs would be less expensive to pursue than funding the construction new US fabrication facilities from scratch, leaving more government funding to be used for developing new technologies that would enable US manufacturers to move up the value chain and gain an enduring advantage. These initiatives would include:

- Support expansion of domestic leading-edge node and legacy chip fabrication capacity by closing the cost differential between overseas and US fabrication operations through tax or regulatory incentives, rather than sponsoring construction of fabrication plants, which should have a viable business case to garner corporate or other private capital.
- Encourage industry leaders TSMC and Samsung to build new US facilities in partnership with US IDMs such as Intel or foundries like Global Foundries using the operational cost incentives described above.
- Incentivize legacy or large-node IC fabrication and packaging in allied countries via tech transfer and purchase agreements with a coalition of IC customers. Corporate or private capital should be available to construct plants provided guaranteed future sales.

- Accelerate “zero-trust” approaches that would enable acquisition of assured electronics from untrusted components.

Although this prong of the proposed strategy would improve resilience and assurance for current chip technologies, it would not constitute a long-term solution. Performance improvements obtained by scaling IC density along the current microelectronics technology's S-curve are decreasing while their costs are simultaneously rising disproportionately. Physical limits such as current leakage and heat generation are beginning to limit the benefits of achieving increasingly small node sizes.⁸⁴

With its recent legislation, the US government has a historic opportunity to steal a march on competitors by exploiting the transition from increasingly dense CMOS chips to new designs that offer specialization, performance, and security. This movement up the value chain would also improve the resilience of the US microelectronics ecosystem by diversifying production through the addition of fabrication and packaging facilities for new chip architectures. However, these opportunities will likely be missed if most US government microelectronics funding goes to building fabrication plants that are unlikely to compete with committed and deep-pocketed foreign rivals.

ENDNOTES

- 1 US Bureau of Economic Analysis, "Industry Economic Account Data: GDP by Industry" (March 25, 2021), <https://apps.bea.gov/iTable/tableViewer?reqid=150&step=2&isuri=1&categories=gdp&xind>.
- 2 Bindya Vakil and Tom Linton, "Why We're in the Midst of a Global Semiconductor Shortage," *Harvard Business Review* (February 26, 2021), <https://hbr.org/2021/02/why-were-in-the-midst-of-a-global-semiconductor-shortage>; Jeanne Whalen, Reed Albergotti, and David J. Lynch, "Biden can't fix the chip shortage any time soon. Here's why," *Washington Post* (March 1, 2021), <https://www.washingtonpost.com/technology/2021/03/01/semiconductor-shortage-halts-auto-factories/>.
- 3 "Study Finds Federal Incentives for Domestic Semiconductor Manufacturing Would Strengthen America's Chip Production, Economy, National Security, Supply Chains," Semiconductor Industry Association (September 16, 2020), <https://www.semiconductors.org/study-finds-federal-incentives-for-domestic-semiconductor-manufacturing-would-strengthen-americas-chip-production-economy-national-security-supply-chains/>; Jeanne Whalen, Jeff Stein and Reed Albergotti, "Growing computer-chip shortage alarms Biden and Congress" (February 23, 2021), <https://www.washingtonpost.com/technology/2021/02/23/biden-semiconductor-shortage-meeting/>.
- 4 "State of the US Semiconductor Industry," Semiconductor Industry Association (June 2020), <https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf>.
- 5 National Highway Traffic Safety Administration, "2020 listings of US/Canada content, averaged by manufacturer," https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/2020_aala_alpha_1-26-21.pdf.
- 6 Kathrin Hille, "TSMC: How a Taiwanese chipmaker became a linchpin of the global economy" (March 24, 2021), <https://www.ft.com/content/05206915-fd73-4a3a-92a5-6760ce965bd9>.
- 7 Thomas Alsop, "Leading semiconductor foundries revenue share worldwide from 2019 to 2021, by quarter," *Statista* (March 8, 2021), <https://www.statista.com/statistics/867223/worldwide-semiconductor-foundries-by-market-share/>.
- 8 Keith Jackson, "Semiconductors are the engine of the global economy—and America isn't making enough of them," *Fortune* (June 30, 2020), <https://fortune.com/2020/06/30/america-tech-semiconductor-manufacturing-investment/>.
- 9 Antonio Varas, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug, "Strengthening the Global Semiconductor Supply Chain," Boston Consulting Group and Semiconductor Industry Association" (April 2021), https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report_Strengthening-the-Global-Semiconductor-Supply-Chain_April-2021.pdf; Ionut Arghire, "Vulnerabilities in Qualcomm Chips Expose Billions of Devices to Attacks," *Security Week* (August 10, 2020), <https://www.securityweek.com/vulnerabilities-qualcomm-chips-expose-billions-devices-attacks>.
- 10 Antonio Varas, Raj Varadarajan, Jimmy Goodrich, Falan Yinug, Strengthening the Global Semiconductor Supply Chain, Boston Consulting Group and Semiconductor Industry Association, April 2021, https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report_Strengthening-the-Global-Semiconductor-Supply-Chain_April-2021.pdf.
- 11 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395, 116th Cong. (January 1, 2021), <https://www.congress.gov/bills/116/congress-house-bill/6395/actions?q=%7B%22search%22%3A%5B%22national+defense+authorization%22%5D%7D&r=6&s=3>. Endless Frontier Act, S. 1260, 117th Cong. (May 28, 2021), <https://www.congress.gov/congressional-record/2021/05/28/senate-section/article/S3915-6>.
- 12 A semiconductor is an element or compound that can carry electrical current but requires higher voltages to do so compared to conductors like copper, aluminum or other metals. In contrast, insulators like plastic, rubber, or gases like helium require very high voltages to pass a current and often mechanically fail in the process. See Karl Hess, *Advanced Theory of Semiconductor Devices* (New York: Wiley, 2000).
- 13 Keith Brindley, "Analog Integrated Circuits," *Starting Electronics*, 4th ed. (Oxford, UK: Newnes, 2011), <https://doi.org/10.1016/B978-0-08-096992-3.00009-3>.
- 14 IEEE, "More Moore," IRDS - International Roadmap for Devices and Systems 2020 Edition, updated in 2020, https://irds.ieee.org/images/files/pdf/2020/2020IRDS_MM.pdf.
- 15 Thomas Alsop, "DRAM manufacturers revenue share worldwide 2011-2021, by quarter," *Statista*, May 12, 2021, <https://www.statista.com/statistics/271726/global-market-share-held-by-dram-chip-vendors-since-2010/>.
- 16 Chaim Gartenberg, "Apple's first-gen M1 chips have already upended our concept of laptop performance," *The Verge* (November 19, 2020), <https://www.theverge.com/2020/11/19/21574057/apple-m1-chips-laptop-performance-intel-qualcomm-competition>.
- 17 James Hayes, "Deep as chips: the new microprocessors powering AI," *Engineering and Technology*, November 11, 2020, <https://eandt.theiet.org/content/articles/2020/11/deep-as-chips-the-new-microprocessors-powering-ai/>.
- 18 Mike Brogioli, "The DSP Hardware/Software Continuum," in *DSP for Embedded and Real-Time Systems*, ed. Robert Oshana (Oxford, UK: Newnes, 2012), 103-111, <https://doi.org/10.1016/B978-0-12-386535-9.00006-8>.
- 19 Peter Wilson, "Digital Circuits, in *The Circuit Designer's Companion*, 4th ed., ed. Peter Wilson (Oxford, UK: Newnes, 2017) 259-320, <https://doi.org/10.1016/B978-0-08-101764-7.00006-2>.
- 20 IEEE, "More Moore," https://irds.ieee.org/images/files/pdf/2020/2020IRDS_MM.pdf.
- 21 Chiplets can also enable disaggregated chip designs in which the final configuration is unknown to foundries and ATP firms, and is only known to the customer which integrates the IC into their system. See DARPA, "A DARPA Approach to Trusted Microelectron-

ics: A Technology-Enabled Trust Approach,” Defense Advanced Research Projects Agency, https://www.darpa.mil/attachments/ATrustthroughTechnologyApproach_FINAL.PDF.

- 22 Semiconductor Engineering, “System on a Chip (SoC),” Knowledge Center, https://semiengineering.com/knowledge_centers/integrated-circuit/ic-types/system-on-chip/; Tim Simonite, “To Keep Pace With Moore’s Law, Chipmakers Turn to ‘Chiplets,’” *Wired* (November 6, 2018), <https://www.wired.com/story/keep-pace-moores-law-chipmakers-turn-chiplets/>.
- 23 William Y. Jiang, X. Quan, and S. Zhou. “Historical, Entrepreneurial and Supply Chain Management: Perspectives on the Semiconductor Industry” *International Journal of Innovation and Technology Management* 07, no. 01 (2010): 1-18, <https://doi.org/10.1142/S0219877010001805>.
- 24 Semiconductors Industry Association, “Study Identifies Benefits and Vulnerabilities of Global Semiconductor Supply Chain, Recommends Government Actions to Strengthen It,” SIA (April 1, 2021), <https://www.semiconductors.org/study-identifies-benefits-and-vulnerabilities-of-global-semiconductor-supply-chain-recommends-government-actions-to-strengthen-it/>.
- 25 Michael S. Malone, *The Intel Trinity: How Robert Noyce, Gordon Moore, and Andy Grove Built the World’s Most Important Company* (New York: Harper Business, 2014).
- 26 Kathrin Hille, “TSMC: How a Taiwanese chipmaker became a linchpin of the global economy” (March 24, 2021), <https://www.ft.com/content/05206915-fd73-4a3a-92a5-6760ce965bd9>.
- 27 George Calhoun, “Intel, Nvidia, Et Al., And American Semiconductor Hegemony,” *Forbes* (August 2, 2020), <https://www.forbes.com/sites/georgecalhoun/2020/08/02/intel-nvidia-et-al-and-american-semiconductor-hegemony/?sh=7a5d0600c298>.
- 28 Kif Leswing, “Apple is breaking a 15-year partnership with Intel on its Macs — here’s why,” CNBC, November 10, 2020, <https://www.cnbc.com/2020/11/10/why-apple-is-breaking-a-15-year-partnership-with-intel-on-its-macs-.html>.
- 29 A TrendForce research report on Intel outsourcing (13 January 2021), of which a summary is available at Simon Kuo, “TSMC to Kick off Mass Production of Intel CPUs in 2H21 as Intel Shifts its CPU Manufacturing Strategies, Says TrendForce” TrendForce, (13 January 2021), <https://www.trendforce.com/presscenter/news/20210113-10651.html>.
- 30 Arjun Kharpal, “How Asia came to dominate chipmaking and what the U.S. wants to do about it,” CNBC, April 11, 2021, <https://www.cnbc.com/2021/04/12/us-semiconductor-policy-looks-to-cut-out-china-secure-supply-chain.html>.
- 31 basavraj.t, “Global EDA in Aerospace and Defense Market Research Report 2021 Growth Share, Trends, Opportunities, Outlook & Forecast 2026,” NeighborWebSJ (April 27, 2021), <https://neighborwebsj.com/uncategorized/6048589/global-eda-in-aerospace-and-defense-market-research-report-2021-growth-share-trends-opportunities-outlook-forecast-2026/>; “How ASML became chipmaking’s biggest monopoly,” *The Economist*, (February 27, 2020), <https://www.economist.com/business/2020/02/29/how-asml-became-chipmakings-biggest-monopoly>.
- 32 Anjani Trivedi, “Want a New Factory to Make Car Chips? That’ll Be \$4 Billion, Please,” Bloomberg (February 21, 2021), <https://www.bloomberg.com/opinion/articles/2021-02-21/the-chip-crisis-a-new-fab-to-make-what-cars-need-will-cost-4-billion?sref=5GYNDTFV>.
- 33 “Explainer: Why is there a global chip shortage and why should you care?” Reuters (March 13, 2021), <https://www.reuters.com/article/chips-shortage-explainer-int/explainer-why-is-there-a-global-chip-shortage-and-why-should-you-care-idUSKBN2BN30J>.
- 34 Oscar Mostofi, “Offshore Outsourcing of the United States Semiconductor Manufacturing: Management Approaches and Strategies,” (doctoral study, Walden University, 2018), <https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=5341&context=dissertations>.
- 35 John Villasenor, “Compromised by Design? Securing the Defense Electronics Supply Chain,” Brookings Institution (November 2013), https://www.brookings.edu/wp-content/uploads/2016/06/villasenor_hw_security_nov7.pdf.
- 36 Robert Triggs, “Qualcomm Snapdragon 888 deep dive: Everything you need to know” Android Authority (March 13, 2021), <https://www.androidauthority.com/qualcomm-snapdragon-888-1179156/>.
- 37 American Foundries Act of 2020, S.4130, 116th Cong. (2020), <https://www.congress.gov/bill/116th-congress/senate-bill/4130/text>.
- 38 Varas et al., “Strengthening the Global Semiconductor Supply Chain,” https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report_Strengthening-the-Global-Semiconductor-Supply-Chain_April-2021.pdf.
- 39 KSM Consulting, “AMARO: Automated Microelectronics Analysis & Reporting Optimization,” KSM Consulting (October 29, 2020), https://info.ksmconsulting.com/hubfs/KSMC-AMARO-Brochure.pdf?__hstc=193356855.47dcd372a137f086bfd71266d98b-fb82.1619402108942.1619402108942.1619402108942.1&__hssc=193356855.4.1619402108942&__hsfp=1170371178; Defense Science Board, “Cyber Supply Chain,” Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (April 2017), https://dsb.cto.mil/reports/2010s/DSBCyberSupplyChainExecutiveSummary-Distribution_A.pdf.
- 40 Antonio Varas et al., “Strengthening the Global Semiconductor Supply Chain,” https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report_Strengthening-the-Global-Semiconductor-Supply-Chain_April-2021.pdf.
- 41 Daniel F. Runde and Sundar R. Ramanujam, “Recovery with Resilience: Diversifying Supply Chains to Reduce Risk in the Global Economy,” Center for Strategic and International Studies (CSIS) (2020), accessed April 25, 2021, <http://www.jstor.org/stable/resrep26011>.
- 42 “How TSMC has mastered the geopolitics of chipmaking,” *The Economist* (May 1, 2021), <https://www.economist.com/busi->

ness/2021/04/29/how-tsmc-has-mastered-the-geopolitics-of-chipmaking.

- 43 I. Wagner, "Automotive semiconductor manufacturers' market share worldwide in 2019," Statista (January 25, 2021), <https://www.statista.com/statistics/277966/automotive-semiconductor-manufacturers-global-market-share/>.
- 44 "Explainer: Why is there a global chip shortage and why should you care?" Reuters (March 31, 2021), <https://www.reuters.com/article/chips-shortage-explainer-int-idUSKBN2BN30J>.
- 45 International Trade Administration, "Taiwan - Country Commercial Guide," US Department of Commerce (September 24, 2020), <https://www.trade.gov/knowledge-product/taiwan-market-overview>; Yimou Lee, "Taiwan says China behind cyberattacks on government agencies, emails," Reuters (August 19, 2020), <https://www.reuters.com/article/us-taiwan-cyber-china/taiwan-says-china-behind-cyberattacks-on-government-agencies-emails-idUSKCN25F0JK>; Michael O'Hanlon, "An asymmetric defense of Taiwan," Brookings Institution (April 28, 2021), <https://www.brookings.edu/blog/order-from-chaos/2021/04/28/an-asymmetric-defense-of-taiwan/>.
- 46 John Donnelly, "Pentagon Races to Shore Up Supply Chain Security," Government Tech (April 9, 2021), <https://www.govtech.com/security/pentagon-races-to-shore-up-supply-chain-security.html>.
- 47 Tom DeSchutter, "Verification And Validation Don't Mean The Same Thing," Semiconductor Engineering (May 25, 2017), <https://semiengineering.com/verification-validation-dont-mean-thing/>.
- 48 P. Prinetto and Gianluca Roascio, "Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy," CEUR Workshop Proceedings (2020), <http://ceur-ws.org/Vol-2597/paper-16.pdf>.
- 49 John F. Miller, "Supply Chain Attack Framework and Attack Patterns," Mitre Technical Report, Mitre Corporation (2013), <https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf>.
- 50 Xida Ren, Logan Moody, Mohammadkazem Taram, Matthew Jordan, Dean M. Tullsen, and Ashish Venkat, "I See Dead p0ps: Leaking Secrets via Intel/AMD Micro-Op Caches," University of Virginia, Computer Science Department, <https://www.cs.virginia.edu/venkat/papers/isca2021a.pdf>.
- 51 S. Ray, E. Peeters, M. M. Tehranipoor, and S. Bhunia, "System-on-Chip Platform Security Assurance: Architecture and Validation," *Proceedings of the IEEE* 106, no. 1, 21-37 (Jan. 2018), <https://doi.org/10.1109/JPROC.2017.2714641>.
- 52 TAME Working Group, "TAME: Trusted and Assured MicroElectronics," Working Groups Report (December, 2019), <https://dforte.ece.ufl.edu/wp-content/uploads/sites/65/2020/08/TAME-Report-FINAL.pdf>.
- 53 C. Todd Lopez, "DOD Adopts 'Zero Trust' Approach to Buying Microelectronics," DoD News (May 19, 2020), <https://www.defense.gov/Explore/News/Article/Article/2192120/dod-adopts-zero-trust-approach-to-buying-microelectronics/>.
- 54 Fortune Business Insights, "Semiconductor Market Size, Share & COVID-19 Impact Analysis, By Components (Memory Devices, Logic Devices, Analog IC, MPU, Discrete Power Devices, MCU, Sensors and Others), By Application (Networking & Communications, Data Processing, Industrial, Consumer Electronics, Automotive, Government) and Regional Forecast, 2021-2028," Semiconductor Manufacturers and Electronics, May 2021, <https://www.fortunebusinessinsights.com/semiconductor-market-102365>.
- 55 Thomas Alsop, "Distribution of semiconductor demand by end use worldwide in 2018 and 2019," Statista (June 23, 2020), <https://www.statista.com/statistics/894267/semiconductor-market-share-worldwide-by-end-use/>; "State of the US Semiconductor Industry," Semiconductor Industry Association (June 2020), <https://www.semiconductors.org/wp-content/uploads/2020/06/2020-SIA-State-of-the-Industry-Report.pdf>.
- 56 Nathan Associates, "Beyond Borders: The Global Semiconductor Value Chain," Semiconductor Industry Association (May, 2016), <https://www.semiconductors.org/wp-content/uploads/2018/06/SIA-Beyond-Borders-Report-FINAL-June-7.pdf>.
- 57 Namchul Shin, Kenneth L. Kraemer, and Jason Dedrick, "Value Capture in the Global Electronics Industry: Empirical Evidence for the 'Smiling Curve' Concept," *Industry and Innovation* 19, no. 2 (February 2012): 89-107, <http://dx.doi.org/10.1080/13662716.2012.650883>.
- 58 Clayton Christensen, *The Innovator's Dilemma* (Cambridge, MA: Harvard Business Review Press, 1997).
- 59 DoD is already pursuing some of these technologies; see "A DARPA Approach to Trusted Microelectronics: A Technology-Enabled Trust Approach," https://www.darpa.mil/attachments/ATrustthroughTechnologyApproach_FINAL.PDF.
- 60 Antonio Varas, Raj Varadarajan, Jimmy Goodrich, and Falan Yinug, "Government Incentives and US Competitiveness in Semiconductor Manufacturing," Boston Consulting Group X Semiconductor Industry Association (September, 2020), <https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf>.
- 61 Anton Shilov, "TSMC to Spend \$100B on Fabs and R&D Over Next Three Years: 2nm, Arizona Fab & More," AnandTech, April 2, 2021, <https://www.anandtech.com/show/16593/tsmc-to-spend-100b-on-fabs-and-rd-over-three-years-2nm-arizona-fab-more>.
- 62 Elias Carayannis and Jeffrey Alexander, "Revisiting Sematech: Profiling Public- and Private Sector Cooperation," *Engineering Management Journal* 12, no. 4 (Dec. 2000): 33-42, <https://doi.org/10.1080/10429247.2000.11415091>.
- 63 These technologies and others that offer performance that diverges from today's path toward smaller node sizes are detailed in IEEE, "More Moore," https://irds.ieee.org/images/files/pdf/2020/2020IRDS_MM.pdf.

- 64 Kevin Fogarty, "GaN Versus Silicon For 5G," Semiconductor Engineering (August 15, 2019), <https://semiengineering.com/gan-versus-silicon-for-5g/>; "Nitride Electronic NeXt-Generation Technology (NEXT)," DARPA (n.d.), <https://www.darpa.mil/program/nitride-electronic-next-generation-technology>.
- 65 Antonio Varas et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing," <https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf>.
- 66 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, <https://www.congress.gov/bill/116th-congress/house-bill/6395/actions?q=%7B%22search%22%3A%5B%22national+defense+authorization%22%5D%7D&r=6&s=3>; "DARPA Electronics Resurgence Initiative," DARPA, <https://www.darpa.mil/work-with-us/electronics-resurgence-initiative>
- 67 Varas et al., "Strengthening the Global Semiconductor Supply Chain," <https://www.semiconductors.org/wp-content/uploads/2021/04/SIA-BCG-Report-Strengthening-the-Global-Semiconductor-Supply-Chain-April-2021.pdf>; "More Moore," https://irds.ieee.org/images/files/pdf/2020/2020IRDS_MM.pdf; Michaela Platzer, "Semiconductors: U.S. Industry, Global Competition, and Federal Policy," Congressional Research Service (October 26, 2020), <https://fas.org/sgp/crs/misc/R46581.pdf>; US National Cyberspace Solarium Commission, "Building a Trusted ICT Supply Chain," CSC White Paper #4 (October 2020), <https://drive.google.com/file/d/1efo96fPx5WkOxTiFFY-1r5y3lFqdit00C/view>.
- 68 Lisa Porter, "The U.S. Defense Department's New Thinking on Microelectronics Security," Office of the Under Secretary of Defense for Research and Engineering (September 2019), <https://www.cto.mil/wp-content/uploads/2019/09/dr-porter-microelectronics-security-2019.pdf>.
- 69 Varas et al., "Government Incentives and US Competitiveness in Semiconductor Manufacturing," <https://www.semiconductors.org/wp-content/uploads/2020/09/Government-Incentives-and-US-Competitiveness-in-Semiconductor-Manufacturing-Sep-2020.pdf>.
- 70 Ian King, "Intel Spending Billions to Revive Manufacturing, Chase TSMC," Bloomberg (March 23, 2021), <https://www.bloomberg.com/news/articles/2021-03-23/intel-to-spend-billions-on-manufacturing-revival-taking-on-tsmc?sref=5GYNDTFV>.
- 71 Kam, Mookun and Hyungphil Kang. "A Study of an Effective Offsets Model for Korea." (2013).
- 72 Willy Shih, "GlobalFoundries To Build Secure Chips For Defense Department In Upstate New York," *Forbes* (February 15, 2021), <https://www.forbes.com/sites/willyshih/2021/02/15/globalfoundries-to-build-secure-chips-for-dod-in-upstate-new-york/?sh=6ec6ed905726>.
- 73 IEEE, "More Moore," https://irds.ieee.org/images/files/pdf/2020/2020IRDS_MM.pdf.
- 74 National Academies of Sciences, Engineering, and Medicine, *Strategic Long-Term Participation by DoD in Its Manufacturing USA Institutes* (Washington, DC: The National Academies Press, 2019), <https://doi.org/10.17226/25417>.
- 75 S. Moore, "Morpheus Turns a CPU Into a Rubik's Cube to Defeat Hackers", *IEEE Spectrum*, April 2021, <https://spectrum.ieee.org/tech-talk/semiconductors/processors/morpheus-turns-a-cpu-into-a-rubiks-cube-to-defeat-hackers>
- 76 J. Shealy et al., "Gallium nitride (GaN) HEMT's: progress and potential for commercial applications," 24th Annual Technical Digest Gallium Arsenide Integrated Circuit (GaAs IC) Symposium, 2002, pp. 243-246, doi: 10.1109/GAAS.2002.1049069.
- 77 Ylan Mui, "Trump Administration to Ban Agencies from Directly Purchasing Equipment or Services from Huawei," CNBC (August 7, 2019), <https://www.cnbc.com/2019/08/07/trump-administration-to-unveil-rule-that-bans-equipment-or-services-purchases-from-huawei.html>; "FCC Designates Huawei and ZTE as National Security Threats," US Federal Communications Commission (June 30, 2020), <https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats>.
- 78 Neil Savage, "Google's Quantum Computer Achieves Chemistry Milestone," *Scientific American* (September 4, 2020), <https://www.scientificamerican.com/article/googles-quantum-computer-achieves-chemistry-milestone/>.
- 79 William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, <https://www.congress.gov/bill/116th-congress/house-bill/6395/actions?q=%7B%22search%22%3A%5B%22national+defense+authorization%22%5D%7D&r=6&s=3>.
- 80 Tony Ramm, "Senate approves sprawling \$250 billion bill to curtail China's economic and military ambitions," Washington Post, June 8, 2021, <https://www.washingtonpost.com/us-policy/2021/06/08/senate-china-science-technology/>.
- 81 For example, see Khaled Salah Mohamed, "Approximate Computing: Towards Ultra-Low-Power Systems Design," *Neuromorphic Computing and Beyond: Parallel, Approximation, Near Memory, and Quantum* (Cham, Switzerland: Springer Nature, 2020), 147-166.
- 82 For example, see Hongyang Jia, H. Valavi, Y. Tang, J. Zhang, and N. Verma, "A programmable heterogeneous microprocessor based on bit-scalable in-memory computing," *IEEE Journal of Solid-State Circuits* 55, no. 9 (September, 2020): 2609-2621, <https://doi.org/10.1109/JSSC.2020.2987714>.
- 83 Anton Shilov, "TSMC to Spend \$100B on Fabs and R&D Over Next Three Years: 2nm, Arizona Fab & More," AnandTech, April 2, 2021, <https://www.anandtech.com/show/16593/tsmc-to-spend-100b-on-fabs-and-rd-over-three-years-2nm-arizona-fab-more>.
- 84 Waldemar Nawrocki, "Physical limits for scaling of integrated circuits," *Journal of Physics: Conference Series* 248 (2010): 012059, <https://iopscience.iop.org/article/10.1088/1742-6596/248/1/012059>.

Hudson Institute
1201 Pennsylvania Avenue, Fourth Floor, Washington, D.C. 20004
+1.202.974.2400 www.hudson.org