iqt™ Insights

The National Microelectronics Challenge

February 2021

By Eileen Tanghal, Dr. Yan Zheng,
& Dr. Sarah Sewall

IQT Insights: The National Microelectronics Challenge

Growing U.S. concerns about national microelectronics competitiveness and supply chain security have prompted proposals for government action.[1] This policy brief explains IQT's view that innovation is the key to meeting both competitiveness and security challenges. The paper argues that the nation should address impediments to commercial success in the specific microelectronics technologies that matter most for U.S. security and competitiveness. In so doing, government can better align private sector incentives with the national interest.

IQT recognizes the value of boosting federal research and development and building U.S.-based chip manufacturing facilities. In IQT's assessment, however, it is equally important to support priority technologies (e.g., tooling, packaging) with commercialization support. Government could support the creation of "sandboxes" to help transition federally funded research from lab to market. Additionally, government could invest in emerging companies where the private sector is not funding specific key technologies at a level commensurate with the national interest. This policy brief, written for the non-expert, provides background and analysis (Section I) and recommendations (Section II).

> "The nation must address impediments to commercial success in specific microelectronics technologies that matter most."

IQT is a non-profit strategic investor that helps deliver emerging technologies to multiple U.S. national security agencies. This analysis flows from our role as one of the world's most prolific investors operating at the intersection of national security, technology trends, and the private sector.

Section I. Background and Analysis

Microelectronics are small electronic components (e.g., transistors, inductors, diodes, capacitors) or complex systems (e.g., microprocessors, AI accelerators) which have become vital for powering everything from smart phones to the most advanced military systems. They provide the building blocks of advanced technologies such as artificial intelligence (AI) and biotechnology. The following section provides a brief overview of the evolution of the industry, technology trends, security considerations, and private sector investment gaps related to microelectronics production and supply chain security.

Industry Evolution

The United States pioneered semiconductor research since the early 20th century, but it was not until its widespread use in radar, radios, and later as the heart of computer systems, did semiconductors become nearly synonymous with microelectronics. U.S. firms led the rapidly growing commercial market and dominated it globally for decades. As the role of semiconductors grew, the industry evolved. Today the microelectronics production process – from materials and design to manufacturing and packaging – is disaggregated and highly globalized. A single chip may traverse 70 countries before its production is complete. [2]

The United States still leads the global industry in several key areas, such as the design of chips and specialized manufacturing tooling, that represent the highest end of the value chain and

[1] The FY21 National Defense Authorization Act includes several new microelectronics initiatives, see https://fcw.com/articles/2021/01/01/ndaa-veto-overturned-senate.aspx. The National Security Commission on Artificial Intelligence 2020 Interim Report and Third Quarter Recommendations also offer recommendations on microelectronics, see https://drive.google.com/file/d/1jg9YlNagGI_0rid-HXY-fvJOAejlFIiy/view.

[2] S. Alam, T. Chu, S. Lohokare, S. Saito, M. Baker (2020). *Globality and Complexity of the Semiconductor Ecosystem. Accenture and GSA.* <https://www.accenture.com/_acnmedia/PDF-119/Accenture-Globality-Semiconductor-Industry.pdf>

annual markets of $419B[3] and $100B[4], respectively. The U.S. lead in design has proved critical in keeping U.S. innovation at the cutting edge of technology development. American companies' strength in tooling equipment also has helped constrain the ability of potential adversaries to develop more advanced manufacturing facilities. However, many other countries' firms are increasingly innovative and important in areas of U.S. strength. Moreover, new aspects of microelectronics on which the United States has not previously focused its research or commercial activities, such as packaging and materials, will likely assume greater significance as the industry continues to evolve.

To date, the most significant change to the microelectronics ecosystem is the migration of manufacturing to Asia. In 1990, the United States and Europe produced three-quarters of global capacity.[5] Relative labor costs, differing environmental sensitivities, and government willingness to help fund large capital investment helped shift much of this manufacturing East. A large Asian network of suppliers and services, including fabrication (production of chips), packaging, assembly, and testing has developed.

Fabrication is a particular U.S. concern. Korea and Taiwan host the dominant "merchant fabrication" facilities, with capacity largely reserved for big chip companies. This poses challenges for small design companies, design startups, and chip customers that require only small batches of testing or production. For U.S. companies, overseas manufacturing introduces additional friction as well as security concerns, including the risk of compromising their intellectual property.

U.S.-based company Intel has maintained fabrication facilities dedicated for their own chip production. However, the majority of U.S. chip designers are now "fabless," meaning that they send their designs to be tested and produced by foreign merchant fabs. Large corporations such as Qualcomm, AMD, and Apple easily access these facilities for their million-chip runs, but startups that require small volume runs and companies designing specialized chips often struggle to gain access to production facilities.

China

China undoubtedly will become an increasingly large player in the global microelectronics industry. The Chinese government employs national technology strategies, state spending, intellectual property theft and forced technology transfer, and integration of civilian and military research and development efforts to support its ambitious microelectronics goals. Chinese firms also received the single largest share of global venture financing for microelectronics in 2019, with 40% of investment (at higher average dollar amounts) compared to 25% to U.S. companies and 18% to the U.K. and Europe.[6]

While previous state-led efforts to develop Chinese microelectronics capacity were largely unsuccessful, China is now pursuing the path taken by Japan and Korea, using the development of memory as a stepping stone to create more sophisticated microelectronics products. Market demand will reinforce the state's push to reach self-sufficiency in production by 2025. China buys 53% of the world's chips and relies on foreign countries for approximately 84% of its internal

[3]Gartner: Market Share: Semiconductors by End Market, Worldwide, 2019. Published 6 April 2020. By Andrew Norwood, Jon Erensen, George Brocklehurst, Ben Lee, Alan Priestley, Bill Ray, Roger Sheng, Amy Teng, Joseph Unsworth, Masatsune Yamaji, Juhi Gupta, Anushree Verma, Rajeev Rajput, Kanishka Chauhan, Nolan Reilly

[4] Gartner: Forecast Analysis: Semiconductor Capital Spending and Manufacturing Equipment, Worldwide, Published 14 October 2020.
By Gaurav Gupta (VP Analyst) and Bob Johnson (VP Analyst).

[5] Fitch, Asa; Santiago, Luis. "Why Fewer Chips Say "Made in the U.S.A.", Wall Street Journal, 3 November 2020.

[6] In-Q-Tel analysis January 2018 using Pitchbook data

semiconductor consumption. [7] Although China's other domestic manufacturing facilities are less advanced, China's Semiconductor Manufacturing International Corporation is working toward cutting-edge (7 nanometer node) technology, nipping at the heels of global industry leaders Taiwan Semiconductor Manufacturing Company (TSMC) and Samsung.

In considering the future evolution of the microelectronics industry, it is reasonable to assume that China will continue to improve its technological capabilities, ultimately achieving 5 or 3 nanometer technology. Additionally, the United States should assume that some foreign governments, particularly China, will subsidize national firms in order to hold market share in this critical industry. Both factors highlight the importance of continued U.S. technology innovation.

Technology Trends

The microelectronics industry is on the verge of significant change. For decades, it relied on shrinking transistor sizes to squeeze more integrated circuits onto a silicon chip, doubling performance every two years while reducing costs. This phenomenon, knowns as Moore's Law, enabled the shift from minicomputers to PCs to smart phones and now the cloud. The process began to slow over a decade ago and experts predict that transistor scaling will reach its final, smallest capabilities at the 3 nanometer node around 2022-23. Although additional nodes at 2 nm and 1.4 nm might be possible, there is a great deal of uncertainty around whether these nodes would ever become viable.

Impending physical limitations on the size of a transistor have begun to reshape microelectronics manufacturing. Companies still using CMOS, the predominate technology for digital integrated circuits, are squeezing additional functions into the remaining capacity of a single chip, however, newer manufacturing approaches combine smaller chips. This new approach relies on producing smaller, more specialized chips designed for memory, processing, or functions such as AI. These smaller modular chips – called "chiplets" – can be assembled together during the packaging phase. This evolution in approach suggests that government policies should focus less on supporting the final stages of CMOS evolution than upon more disruptive technologies such as Advanced Packaging.

Security Concerns

The United States has concerns about both the reliability of (i.e., continued access to) the global supply chain and the security of microelectronics components produced overseas. In weighing public policy solutions, issues include the feasibility of replicating manufacturing capacity given the size and scope of the global supply chain, the relative costs and benefits of facilities operated by government versus the private sector, and the degree to which alternative technological approaches could assure the security of components produced overseas. There is no silver bullet to ensure reliability and security of all microelectronics; prioritization and, as is the case in cybersecurity, a layered approach that features continued technology innovation will be essential.

The Department of Defense's main concern is ensuring a steady supply of secure microelectronics components to maintain its legacy systems. DOD consumes a (relatively) small number of different types of chips, which makes production relatively inefficient (akin to the challenges that startups and specialized chip designers face in seeking production for their limited chip runs). DOD operates a number of older manufacturing facilities and uses a Trusted Access Program Office (TAPO) to certify as "trusted" fabrication facilities and component suppliers that meet its security standards. However, commercial fabrication processes have advanced beyond those in

[7] These are 2019 figures. Pete Singer, *"ISS: The 2020 China Outlook"*, Semiconductor Digest, January 28, 2020, https://www.semiconductor-digest.com/2020/01/28/iss-the-2020-china-outlook

DOD-certified facilities. DOD therefore is seeking ways to guarantee reliable and secure cutting-edge production. One approach would be constructing a more advanced dedicated facility in partnership with a credible American firm. However, this could cost upwards of $15 Billion[8] per facility and, given 10-year construction timelines, would no longer represent the cutting edge by the time of operation.

An alternative approach is a government partnership with the private sector to build and operate a facility, ideally one able to accommodate limited runs from U.S. design firms. This would benefit fabless startups and small companies by improving production access and reducing security concerns; a dual-use facility also would help ensure the full utilization of manufacturing capability and thus profitability of the plant. In an encouraging initiative, Taiwan's TSMC recently committed to open a relatively small but cutting edge (5 nanometer) commercial fabrication plant in Arizona in 2024, thanks to a financial partnership with the U.S. government and the state of Arizona.[9] Foreign ownership of U.S.-based manufacturing (whether TSMC or GlobalFoundries) may not fully address security concerns, but it is critical to acknowledge that vulnerabilities are likely to persist even in U.S.-owned manufacturing facilities.

Further, on-shoring capacity may help ensure supply reliability, but it cannot necessarily guarantee component security. In the long run, then, a layered approach to security that assumes zero trust of a given product is required. This must include developing new approaches to assess the relative security of globally or domestically produced components as well as design architectures that mitigate risks.

Innovation is the key for creating new tools and layered processes to secure or validate the security of chips regardless of their origin. Such a "zero-trust security" approach would benefit commercial as well as DOD consumers. Already, DOD and the Intelligence Community have sponsored research to combine state-of-the-art commercial processes with post-processing techniques to ensure chip security. One such effort involved shipping half-completed commercial materials to be completed through a certified secure process. Other research efforts integrated prefabricated and pre-screened chiplets together to create secure products.

Additional research support is needed to accelerate creation of a zero-trust security regime, specifically for DOE, NSF, DOD, and DARPA to produce novel hardware security technologies and for NIST to improve hardware security standardization. Policies can be mutually reinforcing. For example, to ensure there is demand and uptake of hardware security features, the United States might require that devices that collect personally identifiable information also have basic security features such as a hardware root of trust, trusted enclaves, and unique device identification, depending on the application. An independent certification lab for hardware security could be created to ensure that products meet security standards for the United States and its key international partners.

Private Sector Investment Gaps

The United States has long relied upon private sector innovation in the microelectronics industry. Based on current trends, however, private sector investment is inadequate in areas that IQT considers critical for U.S. innovation leadership and commercial strength.

[8] Christian G. Dieseldorff, "Nearly $50 Billion in Fabs to Start Construction in 2020," *Semi*, September 12, 2019, https://blog.semi.org/business-markets-europe/nearly-50-billion-in-fabs-to-start-construction-in-2020

[9] TSMC, "TSMC Announces Intention to Build and Operate Advanced Semiconductor Fab in the United States," *TSMC News Archives*, May 15, 2020, https://pr.tsmc.com/english/news/2033

There is plentiful private sector investment in "fabless semiconductor" companies that design specialized advanced chips because they often offer "exits" (sales or IPOs) that can provide significant returns. However, other specific microelectronics areas that are important from a national competitiveness perspective have been underfunded. For example, design software and the associated intellectual property (reusable circuit designs that can be put together like Lego© blocks to make larger complex chips) offer less attractive returns compared to other software investments. Likewise, microelectronics hardware offers modest returns over longer timeframes, while requiring significant upfront capital investment. This deters private investment, even though hardware remains vital for overall U.S. microelectronics innovation and security.

Tooling – the equipment needed for cutting-edge manufacturing – is an area of particular concern. The United States leads in advanced tooling technologies (along with Dutch manufacturer ASML, the sole producer of advanced lithography (EUV) tools). Notably, export control of tooling has provided leverage over the pace of other nations' advances in manufacturing (and even other nations' export of chips made using advanced U.S. equipment). This is how the U.S. is preventing Huawei from buying certain Application Specific Integrated Circuits (ASICs) from TSMC in Taiwan, although this approach reinforces Chinese determination to develop its own leading-edge chip production.

The future need, which faces a private sector investment shortfall, is next-generation patterning technologies. These include "direct write" tooling, which removes a significant step in the manufacturing process, and novel deposition tools to accommodate new materials such as graphene, carbon nanotubes, organic and compound semiconductors, and others. (As noted earlier, IQT would prioritize new materials, along with zero-trust security verification technology, in any additional research funding). The combination of new tools and materials is likely to be a truly disruptive to the industry and therefore of geopolitical significance as China invests heavily in catching up in current technologies.

U.S. startups that explore these critical opportunities face difficulties raising funds, however. Of the 215 U.S. microelectronics companies that received private funding during 2015-2017, only five were design software firms, eight sold novel tooling equipment, and nine were in semiconductor IP.[10] The private financing landscape may only become more challenging. Over the past decade, foreign capital had been a significant source of funding for microelectronics startups – particularly in later stage financing. In recent years, as the U.S. tightened restrictions on foreign investment, the percentage of foreign financing of U.S. microelectronics firms has shrunk.[11] Today, American venture capital provides a smaller portion of financing for microelectronics than it does for information technology overall. Other sources of funding, including from government entities such as NASA, DOE, DARPA, and NSF, have been crucial for maintaining even the current level of microelectronics startup activity.[12] In sum, there is a dearth of trusted private investment in the microelectronics startups of the greatest potential national security import.

Section II. Recommendations

The U.S. microelectronics industry faces unique challenges and risks falling short in specific areas of innovation that advance the national interest. Government should consider targeted action to address impediments to commercial success in those technologies that matter most for U.S.

[10] In-Q-Tel analysis January 2018 using Pitchbook data
[11] In-Q-Tel analysis January 2018 using Pitchbook data
[12] In-Q-Tel analysis January 2018 using Pitchbook data

security and competitiveness. In so doing, government can better align private sector incentives with the national interest.

IQT recognizes, as discussed in Section I, that proposals to boost research funding and build fabrication facilities can help promote U.S. microelectronics reliability and security objectives. IQT's recommendations below highlight additional needs that have received less attention from policymakers, specifically, i.) creating commercialization infrastructure to help translate U.S. investment in research into products and ii.) investing in emerging companies where private sector funding is not investing at levels commensurate with national security requirements. As explained in Section I, IQT sees tooling and packaging as priorities for greater support.

Commercialization Infrastructure

The innovation pipeline begins with basic research, extends to prototyping and development, and leads to productization, commercialization, and sustainable, successful companies. The United States historically has invested in the early part of the innovation pipeline, providing research funding to national labs, academia, and industry. This research creates intellectual property (IP) that has the potential to help meet government needs and yield other commercial applications as identified by the private sector. Yet, for a variety of reasons, much of this early IP is not successfully commercialized. The challenge of moving IP beyond R&D and through the full pipeline is sometimes referred to as the "valley of death" or "crossing the chasm." To fully realize its initial investment in research and development, the United States must take steps to support commercialization efforts later in the pipeline, helping research investments lead to viable products and businesses.

Microelectronics companies face some unique hurdles – in particular, gaining affordable access to small production runs that enable the creation and adaptation of prototypes that fit market needs that can attract private capital. The creation of facilities and communities to help address these hurdles will not only help realize research investments and move technology across the chasm to products, it will unleash private capital in support of this process and promote the continuous innovation required in this dynamic industry.

Supportive infrastructure – which can be created via a public-private partnership – should engage both industry and academia, promote interdisciplinary work, provide access to advanced commercial equipment to replicate industry requirements, and enable feedback loops from commercialization back to research. The United States needs commercialization infrastructure for both the front and back ends of the microelectronics production process.

- **Tooling and Bespoke Production**
  A national facility to field innovative semiconductor tools and fabricate next-generation microelectronics products in areas critical to national security would help speed innovation and unlock private investment. Variations on this idea have been called a microelectronics commons, a national semiconductor center, a Lab-to-Fab facility, and a hardware "sandbox." Such a facility could provide researchers and firms hands-on access to production lines that mirror commercial lines and can be adapted to explore new tooling capabilities, materials, components, and processes. The facility could also allow innovators to test and develop security assurance technologies on various devices and process flows.

  A fabrication sandbox could be a win-win proposition in which startups gain access to commercial equipment and tools, early design validation, and valuable testing data to share with potential investors while the government gains early access to innovative

technology that could be tested against government requirements and inform future mission planning and acquisition needs.

- **Advanced Packaging**
  The United States is not a leader in traditional packaging – the end of the production process in which bare chips (called dies) are mounted then wired up through a last layer of electrical connections and enclosed for protection. Yet next-generation packaging is gaining importance as a high-value step because semiconductor functionality is increasingly derived from the packaging process in addition to what's on the chip itself. As Moore's law ends, manufacturers will no longer squeeze more functions onto a single general-purpose chip, but opt to create custom-built chips by integrating various smaller function-specific chiplets instead. Advanced Packaging, in which chiplets of varied and next-generation materials and process technologies can be combined in three dimensions instead of two, is the future of microelectronics customization.

  The significant costs of creating packaging facilities mean that American industry is unlikely to move into this critical innovation space without support from the government. A dedicated facility could test how U.S. chip designs work with Advanced Packaging processes and accelerate the transfer of technology from the lab, helping propel U.S. companies toward leadership in this emerging field. Compared to a leading-edge CMOS foundry, an advanced packaging facility will greatly impact how microelectronics will be designed in the future while costing orders of magnitude less.

Investment Fund

The follow-on challenge within the innovation pipeline is successful formation and scaling of a commercial enterprise.

Market forces may be insufficient to help companies succeed, even when that success serves the national interest by virtue of the technology. The robust U.S. private equity ecosystem will fund companies where there is a demonstrated market opportunity in the form of revenue traction and the potential to build value. However, in critical microelectronics niches, U.S. innovation is dwindling because the commercial returns are no longer sufficiently attractive to private investors. 2019 data show the U.S. trailing China in both the number of hardware companies receiving investment and the mean size of those investments. Furthermore, the private equity and venture community form a much smaller subset of U.S. investors in hardware than in the overarching IT industry. While dual-use commercial technology is critical to the nation's security, responsibility for funding should not rest solely on the shoulders of either private industry or government.

The government needs its own investment vehicles to fill the gaps in the private equity ecosystem where the technologies are of national importance. The United States should establish a Microelectronics Investment Fund targeting key areas such as toolsets, advanced packaging, and origin-agnostic security technologies. These investments would help ensure that essential and disruptive technologies receive early funding, and hopefully catalyze private sector investment by helping de-risk the opportunity. The fund entity would also serve as a central hub for the government to coordinate with the startup community in important dual-use technologies. Even a relatively modest fund of $250 million over five years could accelerate U.S. microelectronics innovation in the areas of greatest relevance to the national interest.

Examples of companies offering products important for U.S. competitiveness or security but facing difficulties raising capital include:

- "Direct write" of the semiconductor circuit. Unlike traditional photolithography tools that need a special laser and a large number of photomasks to create the designed pattern, this company uses an array of electron beams to directly draw custom patterns without needing any masks.
- Fully automated optical inspection system for analyzing opaque, transparent, and semi-transparent materials for features and defects. The company combines their tool with computer vision capabilities to identify manufacturing issues and potentially malicious insertions at the nano or macro level more rapidly than manual quality control methods.
- "Lego® blocks" approach to assemble chiplets into custom chips in a fraction of the time current processes require.
- Security processor for embedded systems that prevents the exploitation of software vulnerabilities at the hardware level and monitors instructions executed from a host processor to ensure that it complies with a set of security, privacy, safety, or customized micropolicies.

In addition to creating an investment fund, government can support commercialization through other policies. Government might create platforms to systematically midwife potential new companies from promising ideas emerging from national research centers (IQT is doing this through IQT Emerge, a new effort focused on commercializing technology innovation from U.S. government-funded R&D initiatives). Agencies could streamline government procurement processes to become a better customer for promising startups. The United States could launch technology challenges to advance solutions to specific issues like opening up the 5G Radio Access Networks or promoting hardware security.

Conclusion

Microelectronics remain vital in both civilian and national security spheres; they are building blocks of consequential emerging technologies like AI and biotechnology. The United States need not become self-sufficient or dominant in every aspect of microelectronics. But sustaining leadership in areas of significance, like chip design and tooling, and developing new approaches, such as Advanced Packaging using new materials, will help keep the United States poised to disrupt the industry. This is more urgent as a strategic competitor marches toward existing cutting-edge technology standards. Where the market will not ensure that leadership or disruption, government should consider policies to align private sector incentives with the national interest.

Many microelectronics policy proposals recommend doing more of what the United States has done historically in funding R&D and supporting secure fabrication facilities. IQT sees great possibility in new approaches to promote the commercialization process and address investment gaps. Sustaining a U.S. lead in key areas of microelectronics demands continuing innovation in areas that the market may not currently value. The government has an opportunity and responsibility to help shepherd the most critical technology beyond research and through early commercialization that the private sector can then move forward as market forces come into play.

-- Learn more about IQT at www.iqt.org. --