Semiconductors and National Defense: What Are the Stakes?

Photo: golibtolibov/Adobe Stock

Commentary by **Sujai Shivakumar** and **Charles Wessner**
Published June 8, 2022

All major U.S. defense systems and platforms rely on semiconductors for their performance. Consequently, the erosion of U.S. capabilities in microelectronics is a direct threat to the United States' ability to defend itself and its allies. Moreover, the U.S. civilian economy is deeply dependent on semiconductor-based platforms for its daily operations. Ensuring U.S. leadership in semiconductor technology and securing the integrity of the value chains that design, manufacture, package, and distribute these chips are perhaps the preeminent economic and national security concerns of the modern era.

TSMC-1135
U.S. Patent 7,923,764

Of course, U.S. leaders have recognized the nexus between semiconductors and national security for decades. In the mid-1980s, President Reagan articulated the need to retain U.S. global leadership in chips to counter the Soviet bloc's numerically superior military forces through "smart" systems driven by semiconductors—satellites, stealth aircraft, cruise missiles, and the like. Today, the United States faces an even greater challenge—it is confronted by a geopolitical rival that is stronger economically and technologically than the Soviet Union ever was. At the same time, the United States is struggling to halt and reverse the loss of its leading capabilities in manufacturing microelectronics. The recent shortage of automotive chips has driven home the damage that the steady erosion of capabilities in chip manufacturing can inflict on the U.S. civilian economy. It is equally important to appreciate the national defense implications of recent adverse trends.

The current chip legislation, which at this writing is pending reconciliation in Congress, represents the most comprehensive program of federal support ever undertaken to ensure the viability of a domestic semiconductor industry—that is, an industry whose critical functions are located within the geography of the United States. The legislation is both essential and overdue. Despite the dwindling number of critics who oppose the legislation as "industrial policy," federal measures to ensure the existence of a robust domestic commercial semiconductor industry—as President Reagan recognized long ago—are vital to U.S. national defense and to the strength and resilience of the U.S. national economy.

Declining Onshore Capabilities

In terms of onshore capability, the U.S. semiconductor industry now has significant gaps in its production chain. The United States remains the unchallenged world leader in semiconductor design, controlling about 85 percent of the world market for electronic design automation (EDA) tools, which are necessary for the design of the most advanced chips. However, there are factors to consider, such as:

- U.S.-based chip manufacturing has declined to around 10 percent of the world total and lacks the onshore capability to make the most advanced devices at the seven- and five-nanometer (nm) nodes. U.S. firms depend on sources in Taiwan and South Korea for production of their most sophisticated designs.

- The United States has very little onshore capability for the outsourced assembly, testing, and packaging (OSAT) of semiconductor devices, holding less than a 5 percent share of these essential functions, with most OSAT operations conducted in Taiwan, China, and Singapore.

- The disaggregation and offshoring of significant elements of the U.S. semiconductor production chain heightens risks relevant to national security, including the potential for intellectual property theft, the introduction of counterfeit devices, and the disruption of the far-flung and delicate chip supply chain by natural disasters or geopolitical conflicts.

AI Challenge from China

These production chain gaps are problematic from a U.S. national security perspective. China has emerged as a major strategic challenger to the United States and is investing heavily in developing its military power and defense industrial base, placing a priority on overtaking the United States and its allies in semiconductor technology. As an independent commission established by Congress recently concluded: "If a potential adversary bests the United States in semiconductors over the long term or suddenly cuts off U.S. access to cutting-edge chips entirely, it could gain the upper hand in every domain of warfare." U.S. vulnerability is particularly acute with respect to the most advanced chips currently in production, which are essential to the creation and application of artificial intelligence (AI)—intelligence generated by machines—which is expected to revolutionize warfare.

China's leaders have set a goal to build a "fully modern" military by 2027 based on "informatization," "intelligentization," and "mechanization," investing heavily in technical areas which support such an approach, such as AI, quantum computing, hypersonics, and microelectronics. AI enables computer systems to solve problems and address tasks that normally require human intelligence, ultimately at speeds and performance levels that vastly exceed those of humans. In the words of the Japanese National Institute for Defense Studies: "As AI does not get fatigued, does not forget, and has no emotional fluctuation, AI is expected to be able to help commanders make decisions by processing large quantities of data quickly and accurately." In a future war, according to U.S. Senator Mike Rounds, "defending against AI-capable

adversaries operating at machine speeds without employing AI is an invitation to disaster." Human operators cannot outmatch multiple machines making thousands of decisions per second coordinated across various systems, nor will they be able to counter an adversary's AI-enabled missile attack, strike against communications satellites and infrastructure, or coordinate firepower strikes, drone swarms, cyberattacks, and other twenty-first century threats. For this reason, the U.S. armed forces' current technical edge over all potential adversaries "could be lost within the next decade if they do not accelerate the adoption of AI across their missions." A massive AI-driven Chinese attack could overwhelm U.S. defenses.

AI systems operate on a foundation of interconnected computer hardware driven by cutting-edge semiconductor devices. "Cutting-edge" is a critical term in this context—it is almost impossible to overstate the performance disparity between advanced AI chips and conventional semiconductor central processing units (CPU). The most advanced chips are tens or even thousands of times faster than CPUs in the development of AI algorithms. "An AI chip a thousand times as efficient as a CPU provides an improvement equivalent to 26 years of Moore's Law-driven CPU improvements," according to Georgetown's Center for Security and Emerging Technology. "State-of-the-art AI chips are necessary for the cost-effective, fast development, and deployment of advanced security-relevant AI systems."

The most advanced AI systems require semiconductor chips based on 7 nm to 5 nm design rules, which are not currently manufacturable in the United States. Intel makes field-programmable gate arrays (FPGA), which are incorporated in AI systems, based on 10 nm design rules—a generation behind 7 nm. The company will begin U.S.-based production of 7 nm chips in 2022. Taiwan Semiconductor Manufacturing Co. (TSMC) is building a fab in Arizona which will operate at the 5 nm node beginning around 2024. But by this time, the state of the art is likely to have moved to 3 nm chips, all of which will be made in Taiwan.

Reliance on Taiwan

At present the United States is currently reliant on facilities located in Taiwan for production of the most advanced AI-enabling semiconductors "that power all the algorithms critical for defense systems and everything else." The United States is one

or two generations behind, if not further. As the chair and vice chair of the National Security Commission on Artificial Intelligence (NSCAI) put it in 2021, "We do not want to overstate the precariousness of our position, but given that the vast majority of cutting-edge chips are produced at a single plant separated by just 110 miles of water from our principal strategic competitor, we must reevaluate the meaning of supply chain resilience and security."

Taiwan, a stable democracy, is closely aligned with the United States and its allies in the Pacific Rim and is dependent on somewhat ambiguous security guarantees for its continued existence as a political entity independent of rule by the Chinese Communist Party. Given that reality, there is virtually no possibility that TSMC or the government of Taiwan would willingly restrict or manipulate the flow of advanced chips to its de facto allies, particularly the United States and Japan.

At present, China is two or more generations behind the U.S. semiconductor industry technologically and will find it virtually impossible to leapfrog the United States–unless it can acquire the foreign technology and know how to do so. This is an objective that China is actively pursuing through multiple channels with a vast deployment of resources.

Notwithstanding Taiwan's close alignment with the United States and its allies and China's lagging technological position in microelectronics, the degree of global dependence on semiconductor production facilities in Taiwan for leading edge chips is a major strategic vulnerability. Geopolitical risks are often, and rightly, mentioned in this context. However, natural disasters such as earthquakes, droughts, or pandemics, all of which have occurred in the recent past, could shut down Taiwan's semiconductor production for a protracted period. Also, China might eventually find a way to coerce TSMC or the government of Taiwan into supporting its development of AI chips or supplying those chips to China. In an extreme case, China could take a variety of military actions, which would disrupt production and delivery of advanced chips.

U.S. dependency on Taiwanese production of chips for defense systems extends beyond AI. TSMC makes semiconductors used in F-35 fighters and a wide range of "military-grade" devices used by the U.S. Department of Defense (DOD). Many U.S.

defense systems use field-programmable gate arrays (FPGA) which are similar to commercial versions but introduce certain specific militarily relevant features, such as higher levels of heat and radiation tolerance. The major designers of FPGAs are U.S. firms that depend on Taiwan for much of their production. The U.S. firm Xilinx, for example, invented the FPGA, but most of its semiconductor wafers are manufactured by TSMC and United Microelectronics Co., another Taiwanese firm. The full extent of U.S. reliance on Taiwan for the manufacture of chips for military applications is unknown, but it is an important factor underlying U.S. government pressure on TSMC to move its production of military devices to the United States.

Dependence on production facilities in Taiwan for advanced semiconductor chips also gives rise to vulnerabilities in the U.S. civilian economy that could affect the broader U.S. defense industrial posture. Semiconductors present in the latest Apple smartphones, 5G communications systems, graphics cards, and data center processors are all designed in the United States, but only TSMC has the capacity to manufacture them.

Meeting DOD's Needs

For decades, the U.S. defense establishment has struggled to ensure a secure domestic production base for the semiconductors needed for military applications. However, advances in semiconductor technology are primarily driven by the development of devices for commercial use. For competitive reasons, U.S. chipmakers have opted to move much of the production, assembly, testing, and packaging functions for commercial chips offshore, usually utilizing specialized foreign firms. Over time, some of those foreign companies have developed and refined competencies that significantly exceed those of even the most competitive U.S. firms, TSMC being the most salient example.

DOD launched the Trusted Foundry Program in 2003 to 2004 to ensure a secure domestic production base for chips needed for military applications. That program, based on arrangements with private sector entities, has grown to include more than 75 device makers and other firms providing other specialized functions such as testing and packaging. As of 2021, U.S.-based trusted foundries were producing about 2 percent of the devices used in military systems, generally chips used in secret

programs or for application-specific uses such as radiation-hardened devices for use in space or nuclear conflict. Other chips needed for defense applications have been obtained from the civilian market, so-called commercial off-the-shelf (COTS) devices. However, whether based on trusted foundry-produced or COTS acquisition, reliance on the commercial sector as a reliable source of chips for military applications has proven to be an ongoing challenge, one driven by a variety of factors:

- The pace of technological advance is much faster on the commercial side than on the military end, chronically limiting the government's ability to access, control, and utilize leading edge technology.

- The service lifespan of chips needed by DOD greatly exceeds that of commercial chips, forcing DOD to constantly search for sources of "legacy microelectronics," or obsolete devices that are no longer made by commercial suppliers except through special arrangements with the defense establishment.

- Chip manufacturing processes, which cannot meet all or even most of DOD's requirements. DOD requires some chips that are state-of-the-art and others that are archaic in commercial terms. Some application-specific devices needed by DOD require the use of exotic materials, compounds, and techniques, such as gallium arsenide, gallium nitride, and silicon carbide, which are not used in large-scale silicon-based commercial production. As a result, there are no "one-size-fits-all" manufacturing solutions.

- The volume of U.S. defense chip needs is a tiny fraction of the demand generated by the commercial market, making the small-batch supply of chips for the military unattractive for many commercial producers. As one U.S. commercial producer put it decades ago: "The military is interested in twos and threes. We are interested in infinity."

- The DOD does not have a unitary, department-wide strategy for microelectronics. Acquisition efforts are extraordinarily complex, scattered across the department,

and have proven unable to keep pace with commercial technological developments.

- The DOD's trusted foundry program, which is subject to destabilization by developments in the commercial sector. In 2017, IBM's trusted foundry in East Fishkill, New York, was acquired by GlobalFoundries, which subsequently terminated its development at the 7 nm node, opting instead to produce less advanced chips which were seen as more profitable. This competitive decision probably made sense from the perspective of GlobalFoundries' shareholders, but it has left the defense establishment without any U.S.-based production capability at the seven nm node until Intel's new fab becomes operational, a milestone which will hopefully be achieved by late 2022. Until then, "U.S. national security applications ... remain dependent on the relatively concentrated [foreign] [integrated circuit] production base, especially in Taiwan."

Meeting the Ongoing Challenge

Such complexities underscore the abiding dependency of the U.S. defense establishment on the commercial semiconductor industry. At present, "the Defense Department cannot remain ahead of potential adversaries without access to an expanded pool of technologies developed in the private sector," which, in microelectronics, have been moving offshore for a generation.

The ongoing challenge is to develop effective policies in consultation with industry, supported with substantial resources, and sustained by a bipartisan commitment to reshore and nurture semiconductor manufacturing. This policy objective will face challenges. Not all measures may prove effective or adequate, but the United States needs to adopt the approach of its competitors by recognizing the critical strategic nature of this technology and do whatever it takes to reshore, redevelop, and incentivize a commercially viable U.S.-based semiconductor industry.

Reshoring this dynamic industry is an exceptional goal, one that will require exceptional measures to address the interlocking challenges of state-backed foreign competitors, rapid technological innovation, and extended global supply chains that no longer satisfy U.S. national security requirements. A business-as-usual approach by the government will not be sufficient. A successful effort will require steady and

substantial commitment of significant resources, deployed through a variety of mechanisms backed by empowered, agile institutions able to deploy resources outside the bounds of standard government practice.

Sujai Shivakumar is director and senior fellow of the Renewing American Innovation Project at the Center for Strategic and International Studies (CSIS) in Washington, D.C. Charles W. Wessner is a senior adviser (non-resident) with the CSIS Renewing American Innovation Project.

Commentary **is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).**

© 2022 by the Center for Strategic and International Studies. All rights reserved.

Tags

Technology, Technology and Innovation, and American Innovation

Center for Strategic and International Studies

1616 Rhode Island Avenue, NW

Washington, DC 20036

Tel: 202.887.0200

Fax: 202.775.3199

MEDIA INQUIRIES

Sofia Chavez

Media Relations Manager, External Relations

202.775.7317

SChavez@csis.org

See Media Page for more interview, contact, and citation details.

©2025 Center for Strategic & International Studies. All Rights Reserved.