EVERY CHIP MATTERS

WHY THE U.S. MUST FIGHT BACK AGAINST A LOOMING CHINESE MONOPOLY IN THE LEGACY SEMICONDUCTOR SECTOR

APRIL 2023
# TABLE OF CONTENTS

**EXECUTIVE SUMMARY** .............................................................................................................3
  - The Problem ...........................................................................................................................................3
  - 3 Solutions ..............................................................................................................................................4

**WHAT ARE LEGACY CHIPS? WHY DO THEY MATTER?** ...............................................................5

**U.S. EXPORT CONTROLS HAVE WRONGLY IGNORED CHINA'S LEGACY CHIP PRODUCTION** ........................................................................................................................................6
  - Battlefield Evidence: How Russia is Repurposing Legacy Chips Against Ukraine .........................7

**HOW CHINA COULD DOMINATE THE LEGACY MARKET IF THE U.S. DOESN’T ACT** .................8

**A CHINESE-DOMINATED CHIP MARKET: A RECIPE FOR DISASTER** .............................................9

**SMIC: A CHINESE MILITARY COMPANY ON THE ENTITY LIST IS GAINING STRENGTH** .............11
  - National Security Leaders Say SMIC-Focused Export Controls Are Almost Totally Ineffective ..........12

**RECOMMENDATIONS FOR ACTION** ........................................................................................13

**Endnotes** ...................................................................................................................................15
EXECUTIVE SUMMARY

The Problem

• **U.S. Government Has Abandoned Legacy Chips:** Since 2020, the U.S. government has actively protected “advanced chips” (set at an arbitrary level of 14 nanometers or smaller for export control purposes), but has ignored legacy semiconductors – those that are critical to defense systems, critical infrastructure, automobiles, medical devices, consumer electronics, and other products.

• **Filling the Void, China Moves to Dominate Legacy Chips:** With the U.S. government exclusively targeting China’s advanced chip manufacturing sector, the People’s Republic of China (PRC) – led by SMIC, its national champion working with the Chinese military – is exploiting the U.S. government’s tunnel vision and spending billions to dominate legacy chip manufacturing.

• **Now a Looming Chinese Monopoly Threatens U.S. National Security:** The national security and economic consequences of a Chinese-dominated legacy chip space would be profound:
  
  • The U.S. would potentially be dependent on China for chips essential to various military technologies and critical infrastructure.
  
  • The world would be re-exposed to supply chain vulnerabilities associated with China-based chip production.
  
  • The Chinese Communist Party would have more new conduits for spying on, hacking, and stealing from targets in the West.
  
  • Elements of the CHIPS Act, designed to boost American chipmaking competitiveness and strengthen semiconductor supply chains, would be rendered irrelevant.
  
  • Other dangerous Chinese tech companies such as Huawei would benefit from a stable source of chips (and American companies could very well not).
3 Solutions

1. IMPOSE MEANINGFUL EXPORT CONTROLS TARGETING SMIC AND OTHER PRC LEGACY CHIPMAKERS

The Commerce Department's Bureau of Industry and Security (BIS) must tighten export controls on SMIC and other Chinese chipmakers. It must apply the presumption of denial standard to ensure they cannot leverage American technologies to support the Chinese military and/or control the global legacy chip market. A Chinese military company identified as a national security threat by the U.S. government should not benefit from a lax BIS licensing policy.

2. STRENGTHEN SECTION 5949 OF THE NDAA:

Congress should strengthen Section 5949 of the FY 2023 NDAA to make sure contractors servicing the federal government cannot use Chinese chips in their equipment. Congress should also amend Section 5949 to prohibit chips made by PRC-owned and operated companies in U.S. critical infrastructure.

3. LEVERAGE TARIFFS TO PROTECT U.S. CAPACITY:

The U.S. Trade Representative should impose tariffs to respond to China's predatory practices and defend American national security. Section 301 of the Trade Act of 1974 provides the federal government with the authorities to defend American prosperity and national security. Senator Tom Cotton of Arkansas has likewise called for a precise application of tariffs, which would be useful in heading off a Chinese effort to dump a glut of legacy chips into the global market.
WHAT ARE LEGACY CHIPS?
WHY DO THEY MATTER?

Legacy chips, also known as mature chips, are those which are 14 nanometers in size or larger. They are found in virtually every electronic device. As a new report by Sujai Shivakumar, Charles Wessner, and Thomas Howell at the Center for Strategic and International Studies describes them: “...Legacy chips are involved in the production of most automobiles, aircraft, home appliances, broadband, consumer electronics, factory automation systems, military systems, and medical devices.”

With the growth of 5G-capable technologies and the adoption of “smart” features in everything from televisions to water bottles, the demand for chips of all kinds is poised to explode in the coming years. The consulting firm McKinsey estimates that semiconductors will become a trillion-dollar industry by the end of the decade.

Crucially, the term “legacy” should not imply that those chips are of less importance than leading-edge chips. Quite the opposite: as the pandemic-related chip shortages that constrained the world economy showed, stable supplies of legacy chips are vital to economic and national security importance. Legacy chips are also high-tech in their own right. As the CSIS report continues:

"Despite the name, legacy chips are not stale technology. The connotations associated with terms like 'mature,' 'older,' and 'legacy' are misleading because these categories of chips are constantly being refined for new requirements and applications...Legacy chips are destined to remain highly relevant to emerging industries and technologies far into the future."

DELOITTE IDENTIFIES LEGACY CHIPS AS CENTRAL TO EUROPEAN INDUSTRY

Countries around the world are facing hard questions about the security and stability of their semiconductor supply chains. A Deloitte Insights report from November 2022 commented on Europe's choice:

One of Europe's big choices is deciding which generation of semiconductor technology to focus on. Deloitte believes leading-edge semiconductors will be important in the future, but chips made through older processes will remain critical to multiple core European industries. These include transportation, especially car manufacturing, health care and factories in general.

The report continues:

At a minimum, any European semiconductor strategy should acknowledge that intermediate and trailing node chips will continue to be manufactured for years. They may even be more important for the European economy given the mix of large European industries that rely on chips other than more advanced nodes and relatively small number of European companies that make products that use advanced node chips...Any EU strategy should therefore support all nodes rather than focusing only on advanced."
U.S. EXPORT CONTROLS HAVE WRONGLY IGNORED CHINA’S LEGACY CHIP PRODUCTION

The Bureau of Industry and Security (BIS) is the Department of Commerce unit responsible for ensuring that foreign adversaries cannot use American technologies to create national security risk for the U.S. One of its main tools for achieving its objectives is limiting the export of certain technologies, such as semiconductor manufacturing equipment, bound for Chinese companies. Since 2020, BIS has prevented the export of certain tools which Chinese chipmakers have depended on to manufacture their chips. The overwhelming reason for these controls is to prevent American technologies from supporting the fabrication of advanced semiconductors for the Chinese military’s use.

Unfortunately, U.S. export controls targeting the Chinese semiconductor sector have almost completely focused on the production of leading-edge chips. As Zeyi Yang has commented in the MIT Technology Review, “[T]he US government has been intentional about limiting the impact to advanced chips...[T]he idea is to inflict pain only in selective areas, like the most advanced technologies that may power China’s supercomputers, artificial intelligence, and advanced weapons.”

Focusing only on so-called “advanced” chips is a mistake. Every chip matters for economic and national security. Legacy chips can be devoted to military uses as easily as advanced chips can be – witness how chips repurposed from dishwashers and refrigerators have been found inside Russian equipment recovered on the battlefields of Ukraine.

The applicability of legacy chips for military purposes exposes how, from a national security perspective, the distinction between legacy and leading-edge chips makes little sense. Shivakumar, Wessner, and Howell write:

The term ‘legacy’ is itself a holdover from an era when military applications were a driving force in chip innovation...If the United States is to protect its economy from the impact of Chinese industrial policy, U.S. strategic thinkers can no longer categorize chips as ‘advanced’ or ‘less advanced’ purely in terms of the size of their components. Instead, policymakers must think more carefully about the importance of specialized legacy chips and policies supporting their production and continued innovation.”
If anyone doubts the value of legacy chips, look at Ukraine. A special report from Reuters from last summer found Russia to be using Western chips in weapons in Ukraine:

“The black metal box, as well as other Russian weaponry shown to Reuters, were collected on the battlefield by Ukraine’s military. They contain Russian electronics bearing Cyrillic markings, sometimes handwritten. But many of the most important electronic components inside are microcontrollers, programmable chips and signal processors stamped with the names of American chip-makers...

While some of the more sophisticated Western chips in the Russian weapons have been subject to special export licensing requirements for years, the investigation found that many of the armaments also contain run-of-the-mill computer chips and other components found in consumer products. These are easily obtainable and in many cases aren’t subject to export restrictions.”

“It’s quite simple... Without those U.S. chips, Russian missiles and most Russian weapons would not work.”

- Anonymous senior Ukrainian official

“We have reports from Ukrainians that when they find Russian military equipment on the ground, it’s filled with semiconductors that they took out of dishwashers and refrigerators.”

- Secretary of Commerce Gina Raimondo, at a U.S. Senate hearing
HOW CHINA COULD DOMINATE THE LEGACY MARKET IF THE U.S. DOESN’T ACT

Failing to issue export controls targeting China’s legacy chip production has created risk for the United States. A disproportionate focus of U.S. export control policy on leading-edge chips has primed China to become the world’s top producer of legacy chips. The CSIS authors share this assessment, commenting:

Given the Western embargo on advanced chip technologies to China, most of the new investments will likely be in the production of older (28 nm and above) devices. An unintended consequence of U.S. export controls on advanced chip technology to China may be a wave of state-backed investment leading to overproduction and, potentially, Chinese dominance of global legacy chip production.12

This scenario is not far-fetched. John Lee, an analyst of China’s chip sector with East West Futures Consulting, insists that China’s place in the legacy market is becoming “bigger rather than smaller.”13 In 2022, Chinese foundries, which predominantly produce legacy chips at 28 nanometers or larger, grabbed 10% of global market share for the first time.14

China has already adopted a model of doling out massive amounts to Chinese companies in hopes of them undercutting competitors on price and thus seizing market share in various technology sectors. To wit, government-subsidized Huawei now sells its 5G wares around the world, and China has become the world’s top source for solar panels thanks to Chinese government handouts to its solar industry. China has also shelled out billions in subsidies for semiconductor companies through the Integrated Circuit Industry Investment Fund. TechInsights’ Chip Economist Dan Hutcheson, has warned of China’s potential dominance of the legacy chip sector, “The Chinese could just flood the market with these technologies... Normal companies can’t compete, because they can’t make money at those levels.”15

“The intense focus on the leading-edge sector by the United States and South Korea — absent attention to growing Chinese capacity in legacy chip manufacturing — may open up an undesirable reliance on China.”

- Chris Park, Council on Foreign Relations16
A CHINESE-DOMINATED CHIP MARKET: A RECIPE FOR DISASTER

There are at least five dangers associated with a Chinese-dominated chip legacy chip market:

1. **THE U.S. MILITARY WILL BECOME MORE DEPENDENT ON CHINESE CHIPS:** Former U.S. National Security Adviser Robert O’Brien has sounded the alarm on the dangers of Chinese chips in U.S. national security systems, writing: “The idea that “made in China” chips are embedded in U.S. defense and intelligence systems, national critical infrastructure, and government networks is both absurd and, unfortunately, our reality. A single compromised chip in the right place can provide our adversaries with unfettered access to critical platforms.”

O’Brien’s statement is all the more plausible when we consider the increase in the number of Chinese companies supplying the Pentagon’s contractors. A 2020 study done by supply chain intelligence firm Govini concluded, “From 2010–2019, the number of Chinese suppliers in the Defense Department’s supplier base in the sample Govini assessed increased by a total of 420%, to 655, across numerous critical industries.” With regard to semiconductors specifically, the number of China-based companies participating in the Pentagon’s supply chain increased 364% (65 companies). Chinese components are almost certainly finding their way into American defense systems.

The U.S. military has already suffered from illegal Chinese intrusion into its systems: In 2008, the U.S. Marine Corps in Iraq discovered that Lenovo products containing secretly planted chips were transmitting data to China. “We don’t have any idea how much data they got, but we had to take all those systems off the network,” testified one Marine officer handling the breach. No U.S. government data exists on how many Chinese chips are in U.S. military systems, but why take the risk with a single one?

Should the U.S. military enter into conflict with China in the future, then any supply of chips from China used in the manufacture of American military hardware would almost certainly grind to a halt. American warfighters should not be at the mercy of their adversaries for the technologies they need to fight and win. To this end, a Government Accountability Office report from 2022 noted several semiconductor sector experts who cited “DOD’s need to maintain its existing weapons systems” as a reason to focus U.S. semiconductor industrial policy on producing legacy chips.

2. **THE U.S. CIVILIAN SUPPLY CHAINS WILL BECOME LESS SECURE:** During the pandemic, the world economy suffered mightily, supply chains were in chaos, and inflation skyrocketed as exports from China – including components for semiconductors – slowed to a trickle. Those days gave the world an idea of the pain that could occur in a repeat scenario caused by another pandemic – or geopolitical developments involving China. From Australia, to Lithuania, to the United States, the Chinese government has already demonstrated that it will punish its trade partners for political stances that do not toe Beijing’s party line. Ceding the global legacy chip market to China would give it a powerful economic tool to weaponize against the world. Former Deputy National Security Adviser Matt Pottinger told Reuters that a China-led legacy chip market, “...would give Beijing coercive leverage over every country and industry – military or civilian.”
3. THE CHINESE COMMUNIST PARTY WILL HAVE NEW OPPORTUNITIES TO SPY, HACK, AND STEAL: The Chinese Communist Party’s global campaigns of digital espionage and theft are by now well-known in the West, and governments at all levels are responding. Roughly 60 nations have committed to keep Huawei out of their 5G networks. Various federal agencies have restricted purchases of technologies from Chinese companies such as Lexmark, Lenovo, Hikvision, Huawei, DJI, and other Chinese companies. As China Tech Threat extensively documented in a report from February 2023, five U.S. states have passed laws banning their state governments from entering into contracts to purchase IT equipment from Chinese-owned and operated companies, and another eleven were working on similar legislation at the time of the report’s release.

But the dawning “Internet of Things” era will present massive challenges in stopping the Chinese surveillance state. The Telegraph, a UK newspaper, recently reported that ministers in the British government have been warned that “China has the ability to spy on millions of people in Britain by ‘weaponising’ microchips embedded in cars, domestic appliances and even light bulbs.” A world in which Chinese legacy chips are ubiquitous gives Beijing virtually unlimited conduits through which it can hack, steal from, and spy on Americans.

4. ELEMENTS OF THE CHIPS ACT WILL BE RENDERED IRRELEVANT: According to the Bookings Institution, “The U.S. CHIPS Act has two main goals: increase supply chain resilience and guard against Chinese advancements from a national security perspective.” The United States has devoted at least $2 billion dollars to boost legacy chip production inside the U.S. That money will be wasted and the goals of the CHIPS Act will be unmet if China can become the world’s legacy chip leader.

5. INCREASED NATIONAL SECURITY RISKS THROUGHOUT THE INFORMATION TECHNOLOGY AND COMMUNICATIONS SPACE: An absence of export controls on SMIC will aid the expansion of other dangerous Chinese technology companies. Case in point: SMIC, has close ties to Entity-Listed Huawei, and they may be working together to expand. In December 2021, industry news outlet Tom’s Hardware said the two Entity Listed companies may be teaming up on a fab to make legacy chips: “We can make an educated guess based on Huawei’s $10 billion investment that this will be a fairly advanced 300mm fab, so it will likely be at least 28nm-capable...” Senator Bill Hagerty of Tennessee has also expressed concern about the SMIC-Huawei relationship. The prospect of Huawei having a stable supply of chips, while other companies potentially do not, gives an inkling of the massive competitive advantage that could be within reach for Chinese multinational companies.
SMIC: A CHINESE MILITARY COMPANY ON THE ENTITY LIST IS GAINING STRENGTH

Semiconductor Manufacturing International Corporation (SMIC) is a microcosm for the shortcomings of current U.S. policy. In 2020, the U.S. government blacklisted SMIC from using certain American technologies, determining that the company "may pose an unacceptable risk of diversion to a military end use in the People's Republic of China." There is no doubt about the linkage between SMIC and the Chinese military: James Mulvenon put out a definitive report in August 2020 that served as the basis of the export controls that came that year. Keith Krach, a former Under Secretary of State, recently told EE Times: "SMIC and YMTC are among dozens of Chinese companies, along with thousands of subsidiaries, that pose serious national security threats to the U.S. because they are building semiconductors for their military. They certainly warrant further restrictions."30

Despite that relationship, the licensing policy put in place focused only on SMIC’s ability to make high-end chips, and was insufficient to stop SMIC’s growing power over the legacy chip market. The company recently reported a record $7.2 billion in earnings, a 30% increase in sales for the second year in a row despite ongoing U.S. sanctions and export controls. If American companies or the U.S. military is on the demand side of the equation for those chips, then it is helping fund a company intimately linked to the Chinese military.

SMIC’s current prosperity, combined with U.S. inaction, has emboldened an expansion. With U.S. export controls making it impossible to produce advanced chips, SMIC has announced the construction of four new chip fabrication facilities since 2020. When those come online, it will more than triple the company’s output, estimates Samuel Wang, a chip analyst with the consulting firm Gartner. He said there is a huge ramp up in new chip fabs across China. "All this will start to have an impact from early 2024 and will be full blown by 2027," said Wang, who also noted that a chip supply increase would depress chip prices.

NATIONAL SECURITY LEADERS SAY SMIC-FOCUSED EXPORT CONTROLS ARE ALMOST TOTALLY INEFFECTIVE

The export controls on SMIC issued in 2020 have too big a loophole to be genuinely effective. According to BIS data released by the House Foreign Affairs Committee, between November 9, 2020, and April 20, 2021, BIS approved 91.3% of license applications worth $41.89 billion from U.S. companies asking to sell technologies to SMIC. 8.3% were returned without action, and only 0.5% -- a single license -- were denied. Given SMIC’s ties to the Chinese military, it’s likely that SMIC is leveraging American technologies to make chips that will help the PRC equip its fighting forces.
Multiple national security leaders have called for BIS to close this loophole:

- In March 2022, Sen. Marco Rubio and Rep. Mike McCaul co-authored two letters to Secretary Raimondo expressing this concern, writing, “Although SMIC’s designation on the Entity List is hampering its ability to make the most bleeding-edge semiconductors, it is having little to no effect on its overall production capability.”

- Senator Hagerty has also remarked that “the entities list restrictions on SMIC are phrased too narrowly.”

- Even the export controls for advanced chips are weak: In 2021, Rep. McCaul and Rep. Mike Gallagher wrote to Secretary Raimondo: “Based on public commentary, nearly 95 percent of the tools SMIC needs to make advanced semiconductor chips at or below 10 nanometers can be reused from older generations. In effect, SMIC will not face serious restrictions, because very few tools are ‘uniquely capable’ of producing a certain chip size.”

---

**BIS RUBBER STAMPS LICENSES FOR A COMPANY SUPPLYING THE CHINESE MILITARY**

<table>
<thead>
<tr>
<th><strong>Number of applications from U.S. companies to the Bureau of Industry and Security to sell technology to SMIC, a Chinese chip company supplying the Chinese military,</strong> 11/9/2020-4/20-21</th>
<th><strong>Number of the 206 applications approved or returned without action (a functional approval)</strong></th>
<th><strong>Number of the 206 applications denied by BIS</strong></th>
<th><strong>Value of licenses for American technologies sold to a company China is depending on for its military technology and legacy chip market domination</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>206</td>
<td>205</td>
<td>1</td>
<td>$41.9 BILLION</td>
</tr>
</tbody>
</table>

---

- Despite this gathering threat, the U.S. government has showed little urgency. According to Reuters, the U.S. government was mulling a new crackdown on SMIC as recently as July 2022. The proposed action, however, would not address the threat of legacy chips: “It would also allow the Biden administration to tighten export controls on SMIC’s most advanced factories, while allowing tools to flow to its facilities that make commodity chips for automobiles and everyday consumer electronics.” More recently, when Rep. Delegate Aumua Amata Radewagen pressed BIS Under Secretary Alan Estevez in March 2023 about the prospect of implementing export controls targeting the legacy sector, Estevez demurred, saying only, “We are stopping the most advanced chips from being made in China.”
RECOMMENDATIONS FOR ACTION

“We have a decade of understanding that the Chinese use software and hardware to facilitate malicious cyber activity against us. We have to make sure that our federal government networks and national critical infrastructure assets are free of Chinese-made chips. A voluntary appeal is not going to work.”

- Rear Admiral (Ret.) Mark Montgomery, cyber expert at the Foundation for the Defense of Democracies and former Executive Director of the Cyberspace Solarium Commission

1. IMPOSE MEANINGFUL EXPORT CONTROLS TARGETING SMIC AND OTHER PRC LEGACY CHIPMAKERS:

In October of 2022, the U.S. government imposed restrictions targeting state-backed chipmaker YMTC, justifying them on the grounds of YMTC “posing a significant risk of becoming involved in activities contrary to the national security or foreign policy interests of the United States.” SMIC has already met that criteria because of its involvement with the Chinese military. BIS must tighten restrictions on SMIC by applying the presumption of denial standard for all exports destined for the company and other Chinese legacy chipmakers.

2. STRENGTHEN SECTION 5949 OF THE NDAA:

In 2022, Congress amended Section 5949 of the NDAA to stop the U.S. government from procuring or using any parts, products, or services that include semiconductors manufactured by specific Chinese companies that represent security risks. But, as former National Security O’Brien has also argued, the FY 2023 NDAA should include an expansion of Section 5949 to completely bar federal contractors from using Chinese chips in their equipment. Congress should also amend Section 5949 to prohibit chips made by PRC owned and operated companies from U.S. critical infrastructure.
3. LEVERAGE TARIFFS TO COUNTER CHINA’S PREDATORY PRACTICES AND PROTECT U.S. CAPACITY:

The U.S. Trade Representative should impose tariffs to address China's predatory practices and defend America's national security. The U.S. China Economic and Security Commission notes that Section 301 of Trade Act of 1974 "provides USTR with a great deal of flexibility and can allow for novel remedies." The Commission further notes that Section 301 investigations are "more open-ended"... "leaving a wide range of actions available to the administration." USTR should target PRC chips in products coming into the United States.

Senator Tom Cotton of Arkansas has likewise called for a precise application of tariffs, which would be useful in heading off a Chinese effort to dump a glut of legacy chips into the global market:

"The United States also can use targeted import duties against Chinese exporters that receive substantial state subsidies or engage in anti-competitive practices, such as export dumping. Unlike general tariffs that treat cheaters and rule-followers identically, targeted import duties clearly delineate between actors that compete on fair terms and those that do not. Using import duties in this way would give Chinese firms a clear incentive to play by the rules—while hammering those that do not."
EVERY CHIP MATTERS | APRIL 2023

ENDNOTES

10. Ibid.
34. https://www.reuters.com/technology/china-massive-older-chip-tech-build-up-rises-us-concern-2022-12-13/
EVERY CHIP MATTERS

WHY THE U.S. MUST FIGHT BACK AGAINST A LOOMING CHINESE MONOPOLY IN THE LEGACY SEMICONDUCTOR SECTOR

www.chinatechthreat.com