Semiconductors are a vital underpinning of our modern digital life. The United States and its allies have long been leaders in this technology, yet our adversaries seek to close the gap in innovation leadership and technological acumen. The policies of Beijing to foster their own semiconductor industry and the development of “military-civil fusion” presents a direct threat to the economic prosperity and national security of the United States. The importance of semiconductors, the web of global supply chains, and the need to marshal international cooperation make this a complex challenge for policymakers to address.

In this CSPC Geotech program white paper, CSPC Senior Advisor Andy Keiser analyzes the history of the Chinese semiconductor industry and Beijing’s policies of subsidization, IP theft, industrial espionage, and forced tech transfer—and lays out some recommendations to mitigate this threat.
SECURING THE KEYS TO THE FUTURE: 
COUNTERING THE THREAT FROM STATE-BACKED 
CHINESE SEMICONDUCTOR COMPANIES 

CSPC GEOTECH WHITE PAPER 
By: Andy Keiser
October 2020 

TABLE OF CONTENTS 
Executive Summary ................................................................. 1 
Introduction ........................................................................... 7 
Industry Landscape .............................................................. 8 
  Development of Semiconductor Industry in Adversarial Nations ........................................... 8 
  Chinese Government Industrial Policy ............................................................................ 10 
  National Security Threat of State-Backed Chinese Semiconductor Companies .................. 11 
Policy Response to the Threat ........................................................................ 14 
  U.S. Response ...................................................................... 14 
  Global Response ................................................................... 17 
Recommendations ..................................................................... 19 
Conclusion ............................................................................... 21 

1 Andy Keiser is a Senior Advisor to the Center for the Study of the Presidency and Congress and previously served, among other positions, as a Senior Advisor to the House Permanent Select Committee on Intelligence. Mr. Keiser also conducts cybersecurity consulting and federal lobbying for several companies, including in the telecommunications and technology sectors. 

The views in this paper are of the author and do not imply endorsement by CSPC or its Trustees.
EXECUTIVE SUMMARY

Semiconductors are essential to much of the U.S. economic and national security of the present and future.

The United States and our allies should take immediate action to secure the semiconductor and semiconductor manufacturing equipment (SME) supply chain and prevent reliance on or infiltration by adversarial nations like China.

Introduction

Through its “Made in China 2025” plan, the Chinese Communist Party (CCP) has made it a top priority to wean itself off of Western technology, including semiconductors. Their attempts to capture increased market share and leverage critical supply chains as a geopolitical weapon—combined with their history of utilizing technology to conduct espionage or economic disruption—pose a clear threat to U.S. national security.

Semiconductors were first commercialized via transistors at Bell Labs in New Jersey following World War II in 1948 and the process to manufacture transistors using silicon was perfected by Texas Instruments shortly thereafter. Over time, these transistors and circuits were made onto single chips, which have become gradually smaller and more powerful over time.

Industry Landscape

The United States of America has largely dominated the global semiconductor industry as U.S. military R&D support and product demand led to the explosion of the industry that occurred in the 1970s and 1980s.

More recently, South Korean manufacturers vaulted toward the top of the semiconductor market, while Taiwan, the European Union and Japan remain solid, new entrants from China, backed by the full force of their government, have seen double-digit growth in recent years.

Development of Semiconductor Industry in Adversarial Nations

- Russia
  
  During the 1960s, the then Soviet Union developed microelectronic technologies, including semiconductors, domestically with some success with companies such as Mikron and Angstrem. Though typically lagging the capability and sophistication of their Western adversaries, Soviet chips were serviceable. In recent years, Russia sought to rejuvenate its semiconductor and microelectronic business in an effort to create some independence from the U.S. and its allies, but this effort was stymied by international politics.

- China
  
  During the 1960s, Chinese industry first developed semiconductors and for a period of thirty years the government managed a top-down style that focused on state-planning and reliance on domestic semiconductor producers.
Semiconductor Manufacturing International Corporation (SMIC) was founded in 2000 in Shanghai by an industry veteran who worked in the U.S. and Taiwan. It is now a top five global foundry.

Founded in 2004, HiSilicon is the fabless chipmaker and direct subsidiary of Chinese telecommunications giant Huawei.

In the 2010s, three notable new Chinese-based players were introduced to the global semiconductor scene – ChangXin Memory Technologies (CXMT), Yangtze Memory Technologies Co. (YMTC), and Fujian Jinhua Integrated Circuit Co.

**Chinese Government Industrial Policy**

Beijing’s central planners follow a clear pattern for those key industries they seek to dominate:

First, build technical knowhow through the following means: intellectual property (IP) theft overseas; domestic state-sponsored research and development; acquisition of IP via joint venture or direct investment; requirements forcing Chinese business partners and technology transfers for entry into the Chinese market; and, domestic workforce training and support.

Second, create a robust domestic industry by guaranteeing market share in the world’s second largest economy; transfer stolen IP from the Chinese military and intelligence services to domestic companies; secure access to necessary natural resources, provide lines of credit from state-sponsored financial institutions; and, institute quotas and tariffs on foreign competitors in China.

Third, flood the global market with products at- or below-cost to increase Chinese companies’ global market share and bankrupt foreign competitors, while sustaining said losses through lines of credit from state-sponsored financial institutions.

In addition to seeking leadership in R&D and independence in sensitive technologies, Beijing seeks to maintain interdependence further down the value chain or to increase interdependence through greater financial ties and cross-investment.

**National Security Threat**

- **Military and Intelligence Use**

  Semiconductors are essential components in every nation’s military and intelligence systems including communications systems, satellites, fighter jets, bombers, tanks, and armored personnel carriers.

  The United States Department of Justice brought numerous cases of espionage by Chinese government officials seeking to acquire sensitive U.S. technology and national defense secrets.

  Top Chinese semiconductor producer SMIC maintains close ties to the Chinese military and CCP. One of SMIC’s top customers is Huawei, which is known to have direct ties and a foundation upon the Chinese military and intelligence services. All Chinese-domiciled companies, including Chinese semiconductor companies CXMT and YMTC, are required to
cooperate with the Chinese military and intelligence services under the 2017 National Intelligence Law of the People’s Republic.

Since the collapse of the Soviet Union, Russian government leaders have unsuccessfully sought to rejuvenate its technology sector, including the semiconductor industry, in an attempt to diversify its economy from reliance on energy production. The challenge for Russia, much like their Soviet predecessors, is scale. The Russian domestic market is too small and isolated to support domestic suppliers, and, while Russia may match the West and China in technical acumen, they lack the ability and capacity to produce cutting-edge technologies at scale.

- Telecommunications

Semiconductors are critical components of most modern telecommunications equipment including mobile devices, base stations, and routers. Reliance on these devices creates a vulnerability that forces national security policy makers to prioritize the supply chain security of these technologies, including semiconductors.

- Future technologies

Semiconductors are critical to emerging technologies such as fifth generation wireless technologies (5G), autonomous vehicles, artificial intelligence (AI), and increased Internet of Things (IoT) applications.

Through its “Made in China 2025” plan, China seeks to dominate each of these high-tech areas and the next-generation semiconductors which make them possible.

- Supply Chain Security

Supply chain security is of utmost importance to the Pentagon. Yet a single Senate Armed Services Committee investigation in 2012 found 1,800 cases of counterfeit electronic parts in defense equipment—each case presenting its own potential vulnerability.

Should the domestic semiconductor industrial base collapse, the U.S. military and intelligence services could lose access to the critical, secure supply chains necessary to conduct operations safely and securely.

**U.S. Policy Response to the Threat**

- CFIUS/FIRRMA

American Presidents used the Committee on Foreign Investment in the United States (CIFIUS) five times to block foreign investment transactions since its inception in 1975, three of which impacted the semiconductor industry.

In 2018, Congress approved, and President Donald Trump signed into law legislation targeting CFIUS review of national security risks in new areas including private equity investments and joint ventures acquiring sensitive technologies, including in the semiconductor industry.
• Entity List

In 2018, the United States Department of Commerce Bureau of Industry Security (BIS) added Chinese semiconductor company Fujian Jinhua Integrated Circuit Company, Ltd (Jinhua) to its Entity List in response to theft of intellectual property from U.S.-based Micron.

Last year, BIS added HiSilicon to the Entity List when it expanded Huawei’s listing to all global affiliates.

• Export Controls

In 2018, Congress passed, and the President signed into law the Export Control Reform Act (ECRA). The ECRA sought to restrict exports to China of key foundational and emerging technologies, including semiconductors, citing a national security threat.

In August of 2020, BIS issued its long-awaited advanced notice of proposed rulemaking concerning foundational technologies from ECRA. The notice highlights that the export of semiconductor manufacturing equipment to indigenous modernization efforts in China, Russia, and Venezuela may pose a national security threat.

• “Military End User” Licensure

In September of 2020, the Commerce Department announced to companies doing business with SMIC that they would need to apply for “military end user” licenses—which had not previously been required.

• Counterintelligence

80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice are reported to involve cases that would benefit China.

In 2018, the United States Department of Justice unveiled a new China Initiative “to confront China’s malign behaviors and to protect U.S. technology.”

• Domestic Production Incentives

Senators John Cornyn and Mark Warner have introduced S. 3933, The CHIPS for America Act, which would provide $22 billion in financial incentives and R&D to facilitate domestic semiconductor manufacturing.

Senators Tom Cotton and Chuck Schumer have introduced similar legislation called the American Foundries Act.

• Hong Kong

Following passage of a new national security law extending mainland governance and authority over the previously semi-autonomous region (SAR) of Hong Kong, the Commerce Department extended export controls to China for key technologies, including semiconductors, to the Hong Kong SAR as well.
• International Push

The U.S. Department of State leads an inter-agency initiative to warn allies around the world of the inherent dangers of Chinese military-civil fusion and their growth in key dual-use technologies such as semiconductors.

**Global Policy Response to the Threat**

In 1996, the Wassenaar Arrangement was approved by 33 nations as the first global multilateral arrangement on export controls for sensitive dual-use goods and technologies. Last year, the group updated the pact to include new language on semiconductors and semiconductor manufacturing equipment (SME).

• Netherlands

Media reports indicate that the Dutch government blocked a shipment of an advanced chip-making machine by Dutch SME maker ASML to China-based SMIC.

• Japan

Media reports have indicated that major Japanese semiconductor firms, including Tokyo Electron, would not sell to products to Chinese companies that end up on the BIS Entity List.

Last year, media reports indicated that Japan was considering advanced technology exports controls like what the United States has promulgated focusing on the threat from China.

• India

Following deadly border clashes with China, India has banned 118 Chinese apps. Media reports also indicate that India is moving to restrict Chinese telecommunications companies from building out future domestic telecommunications networks.

• United Kingdom and the European Union

The United Kingdom and several major carriers in European Union countries have reportedly decided to not use Chinese telecommunications giants Huawei or ZTE to build out their 5G networks.

• Taiwan

In response to increased aggression from China, Taiwan has taken a series of steps targeting mainland-based technology companies. The largest semiconductor foundry in the world, Taiwan Semiconductor Manufacturing Company (TSMC), announced that it would not sell its high-end chips to Huawei or HiSilicon.

• South Korea

South Korea decided to both boost its domestic champions and provide some independence from China when it decided to have Samsung and other domestic companies build South Korea’s 5G network. Media reports indicate that both Samsung, SK Hynix and LG Display will cease supplying Huawei with high end components.
Policy Recommendations

• Entity Listing

Should existing measures such as “military end user” licensure and other export controls fail to meet this national security challenge, BIS should add SMIC, CXMT, YMTC and potentially other Chinese-domiciled semiconductor companies as warranted to the Entity List. Sensitive U.S. components should not go to further the military technology of our primary geopolitical competitor.

• Export Controls

BIS should conclude a swift, but thoughtful, interagency rulemaking for its export restrictions of foundational technologies to include high-end semiconductors and SME to the state-owned enterprises of adversarial nations like China and Russia.

• Diplomatic Pressure

The U.S. State Department should continue to lead the interagency on a global diplomatic effort to ensure allies understand the risks of using state-backed Chinese technology. The Department’s Clean Network Initiative programs should be expanded to include semiconductors.

• Incent Domestic Production

Domestic and allied production capacity should be a key consideration for policymakers as they consider policies affecting semiconductor supply chains and their security. To foster domestic capacity and continued U.S. innovation leadership, Congress should immediately approve and the President should sign into law the CHIPS for America Act or something similar to match the massive financial incentives China is pouring into its own state-backed industry, creating a national security threat to the U.S. and our allies.

• Expand Defense Industrial Base to Semiconductor Production

Utilizing the Industrial Base Fund and the Defense Production Act’s Title III financial tools, this would be done in a similar way to how the U.S. Defense Industrial Base protects ship, tank and airplane manufacturing lines, none of which function without high-end semiconductors.

• Prepare for Retaliation

Should the United States take the actions above, we certainly should prepare for relation by the Chinese government to related or potentially unrelated industries, or individuals.
INTRODUCTION

Building off of the Center for the Study of the Presidency and Congress (CSPC) 2019 paper titled “Geotech: Fostering Competitiveness for Technological Competition,” this paper intends to be a deeper examination of semiconductors—their importance to the economy and military of the present and future and the threat adversarial nations’ semiconductor industries and related policies pose to the United States.²

Through its “Made in China 2025” plan, the Chinese Communist Party (CCP) has made it a top priority to wean itself off of Western technology, including semiconductors. Their attempts to capture increased market share and leverage critical supply chains as a geopolitical weapon—combined with their history of utilizing technology to conduct espionage or economic disruption—pose a clear threat to U.S. national security. Though the Russian government has had some past success in the field and maintains interest in developing its industry in the present, the primary threat today looms from the rapidly rising capacity of state-backed semiconductor companies in China.

This report focuses on the importance of silicon semiconductor³ computer chips or integrated circuits as essential components in the fabrication of electronic devices such as televisions, radios, computers, medical devices, and mobile devices that are major features of modern, daily life.⁴

Semiconductors were first commercialized via transistors at Bell Labs in New Jersey following World War II in 1948 and the process to manufacture transistors using silicon was perfected by Texas Instruments shortly thereafter.⁵ Over time, these transistors and circuits were made onto single chips, which have become gradually smaller and more powerful.⁶ The industry has expanded to several countries and is now a $500 billion global industry responsible for 240,000 direct jobs in the United States alone.⁷

There are four main categories of semiconductor computer chips: memory chips, microprocessors, standard chips, and complex systems-on-a-chip. Chips are also divided by types of circuitry: digital, analog, or mixed.⁸ Microprocessing chips serve as the central processing unit (CPU) of a computer or mobile device.⁹ Memory chips include flash, non-volatile memory (NAND), or dynamic random-access memory (DRAM).¹⁰

---

³ Semiconductors are materials that have a conductivity between conductors, typically metals, and non-conductors, such as glass or ceramic.
INDUSTRY LANDSCAPE

The United States of America has largely dominated the global semiconductor industry as U.S. military R&D support and product demand led to the explosion of the industry that occurred in the 1970s and 1980s. Via companies like Intel, the United States leads in microprocessing chips and NAND, and is a leader in DRAM via Micron—though South Korean companies including Samsung and SK Hynix now lead the global DRAM market.\(^\text{11}\)

The 1980s and early 1990s saw the arrival of strong Japanese electronics companies, such as Toshiba and NEC, which led to significant growth in the semiconductor space, propelling them to lead in the DRAM market during portions of those decades. However, from the mid-1990s until recently, the United States retook the overall leading position largely due to the rapid growth of a market for PCs and smartphones. This market is dominated by U.S. chip manufacturers such as Intel and Micron, and fabless semiconductor companies like Qualcomm, Broadcom, Nvidia, and AMD—companies designing their own chips and procuring them from other fabricators, or fabs.\(^\text{12}\)

More recently, South Korean manufacturers vaulted toward the top of the semiconductor market, while Taiwan, the European Union and Japan remain solid. New entrants from China, backed by the full force of the government, have seen double-digit growth in recent years.\(^\text{13}\)

The countries and companies identified above invest more than $70 billion total annually in research and development of next-generation semiconductors.\(^\text{14}\)

Development of Semiconductor Industry in Adversarial Nations

- **Russia**

  During the 1960s, the then Soviet Union developed microelectronic technologies, including semiconductors, domestically with some success from companies such as Mikron and Angstrem. Though typically lagging the capability and sophistication of their Western adversaries, Soviet chips were serviceable. A major part of Soviet semiconductor development was enabled by espionage from the Soviet intelligence services. A now-declassified 1982 CIA report highlights semiconductors as a “major field of interest to Soviet and Eastern European visitors to the United States.”\(^\text{15}\) Over time, the Soviet Union’s and then Russia’s domestic semiconductor industry weakened due to lack of innovation and imports from abroad.

---


\(^{14}\) Supra note 4.

In recent years, Russia sought to rejuvenate its semiconductor and microelectronic business in an effort to create some independence from the U.S. and its allies, but this effort was stymied by international politics and limitations in their industries’ ability to produce high-tech components at scale. For example, Angstrem had begun developing new, sophisticated chips but this effort was severely hampered by U.S. sanctions prohibiting key imports in response to Russia’s annexation of Crimea in Ukraine.16

➢ China

During the 1960s, Chinese industry first developed semiconductors, and, for a period of thirty years, the government managed a top-down style that focused on state-planning and reliance on domestic semiconductor producers. That changed in the 1990s when the industry began partnering with foreign companies via joint ventures and found some mixed success.17

Semiconductor Manufacturing International Corporation (SMIC) was founded in 2000 in Shanghai by an industry veteran who worked in the U.S. and Taiwan. It is now a top five global foundry.18

In the 2010s, three notable new Chinese-based players were introduced to the global semiconductor scene. Created as a “pilot project of the Made in China 2025” initiative, ChangXin Memory Technologies (CXMT) grew to become a player in the DRAM market while Yangtze Memory Technologies Co. (YMTC) saw major growth in NAND. Fujian Jinhua Integrated Circuit Co. rapidly became major producer of DRAM before shutting down following U.S. action to restrict their access to U.S.-made components.19

Founded in 2004, HiSilicon is the fabless chipmaker and direct subsidiary of Chinese telecommunications giant Huawei. HiSilicon exclusively provides chips both for Huawei’s network infrastructure and its mobile device businesses.20

The recent, rapid growth of the indigenous Chinese semiconductor industry drew the attention of global policymakers worried about supply chain security, their own domestic industry and China’s rise and their predatory practices.

18 Id.
Chinese Government Industrial Policy

CCP leadership seeks independence from its global adversaries in the West, including from the key technologies of the future it intends to dominate. The fact that China consumes more than 50 percent of the global semiconductor market but only produces five percent adds extra urgency for CCP central planners. The “Made in China 2025” plan builds off earlier industrial plans to become 70% reliant on domestic companies by 2025 for key technologies and seeks a dominant position by 2049 – the 100 year anniversary of the successful CCP revolution. In the past ten years, the CCP released 100 separate plans identifying development of the domestic semiconductor industry as a key objective.

Beijing’s central planning follows a clear pattern for those industries they seek to dominate:

- First, build technical knowhow through the following means: intellectual property (IP) theft overseas; domestic state-sponsored research and development; acquisition of IP via joint venture or direct investment; requirements forcing Chinese business partners and technology transfers for entry into the Chinese market; and, domestic workforce training and support.
- Second, create a robust domestic industry by guaranteeing market share in the world’s second largest economy; transfer stolen IP from the Chinese military and intelligence services to domestic companies; secure access to necessary natural resources, provide lines of credit from state-sponsored financial institutions; and, institute quotas and tariffs on foreign competitors in China.
- Third, flood the global market with products at- or below-cost to increase Chinese companies’ global market share and bankrupt foreign competitors, while sustaining said losses through lines of credit from state-sponsored financial institutions.

CCP leaders announced they intend to follow the same playbook in advanced technologies such as semiconductors. A recent investigation found that Chinese government-backed hackers compromised at least seven Taiwanese chip firms, while news reports indicate that

Beijing is preparing broad support for so-called third generation semiconductors for the five years through 2025...A suite of measures to bolster research,

---

23 Supra note 13.
In total, some experts believe that “China plans to invest $1.4 trillion over the next decade to develop a ‘closed-loop semiconductor ecosystem’ that would eliminate U.S. chip exports by 2035.” Though Chinese firms enjoyed the most success in memory chips—NAND and DRAM, they are likely only a few years away from being able to competitively produce the most advanced chips.

In addition to seeking leadership in R&D and independence in sensitive technologies, Beijing seeks to maintain interdependence further down the value chain or to increase interdependence through greater financial ties and cross-investment. Whether this is to promote transpacific commerce and investment or to weaponize the interdependence in supply chains is left to the eye of the beholder. This creates a challenge for policymakers, as the U.S. semiconductor industry and U.S. consumer electronics companies have close commercial ties with their Chinese counterparts. As measures to counter Chinese threats to U.S. national security are implemented, government and the private sector should maintain dialogue about these measures—and, specific to this sector, impacts on international supply chains and semiconductor fabrication capacity.

National Security Threat of State-Backed Chinese Semiconductor Companies

- **Military and Intelligence Use**

  Semiconductors are essential components in every nation’s military and intelligence systems including communications systems, satellites, fighter jets, bombers, tanks, and armored personnel carriers.

  A proposed rule by the U.S. Commerce Department’s Bureau of Industry and Security (BIS) in August of 2020 notes “items including semiconductor manufacturing equipment…can be tied to indigenous military innovation efforts in China, Russia or Venezuela. Accordingly, they may pose a national security threat.”

---


The U.S. Department of Justice brought numerous cases of espionage against Chinese government officials uncovered stealing sensitive U.S. technology and national defense secrets. In one 2019 conviction, University of California, Los Angeles (UCLA) professor Yi-Chi Shih was convicted of sending sensitive semiconductor chips with military applications to Chinese government military contractors.

The semiconductor chips at the heart of this case were shipped to Chengdu GaStone Technology Company (CGTC), a Chinese company that was building a [Monolithic Microwave Integrated Circuits or MMIC] manufacturing facility in Chengdu. Shih was the president of CGTC, which in 2014 was placed on the Commerce Department’s Entity List, according to court documents:

Due to its involvement in activities contrary to the national security and foreign policy interest of the United States—specifically, that it had been involved in the illicit procurement of commodities and items for unauthorized military end use in China.

According to Michael Elleman, director of the nonproliferation and nuclear policy program at the International Institute for Strategic Studies’ Americas division, MMICs provide the underlying data needed for acquiring enhanced targets, and providing data-rich high-speed, secure communications that can jam or spoof enemy radars or communications.

Top Chinese semiconductor producer SMIC maintains close ties to the Chinese military and CCP. Testing and technology transfers are common between SMIC, defense contractors, and other state-owned technology providers. People’s Liberation Army (PLA) and defense industrial base researchers use SMIC chips and processes directly in their research, including for aerospace and military applications. The shareholders of SMIC are a “who’s who” of the Chinese military industrial and research universe, with close ties to top CCP leadership and key core functions.

One of SMIC’s top customers is Huawei, which is known to have direct ties and a foundation to the Chinese military and intelligence services. All Chinese domiciled companies, including Chinese semiconductors companies SMIC, CXMT and YMTC, are required to cooperate with the Chinese military and intelligence services under the 2017 National Intelligence Law of the People’s Republic. Article seven of that law states: “Any organization or citizen shall support, assist and cooperate with the state intelligence work.” On a broader political scale, Xi Jinping

37 Id.
and the CCP promise entrepreneurs and business leaders profits, but only if they cooperate with the party’s goals, leadership, and security. This military-civil fusion and the politicization of corporate decision-making demonstrate the little independence the private sector has from the state in China, unlike in democratic nations.

Russia’s semiconductor industry was developed in the 1960’s to supply the Soviet military. Companies Mikron and Angstrem maintained close ties to the Soviet Communist Party and government leadership. In 1981 Angstrem received the Order of the October Revolution, which was given “for services furthering communism or the state, or in enhancing the defenses of the Soviet Union, military and civil.”

Following the collapse of the Soviet Union, Russian government leaders sought to rejuvenate its technology sector, including the semiconductor industry, in an attempt to diversify its economy from reliance on energy production. These efforts failed multiple times due to lack of technical expertise, robust foreign competition, difficulties achieving scale production of high-tech components, and Western sanctions responding to malign Russian activity.

- **Telecommunications**

  Semiconductors are critical components of most modern telecommunications equipment including mobile devices, base stations, and routers. Thirty-three percent of all semiconductors made are devoted to communications equipment, including networking equipment and radios in smartphones.

  Reliance on these devices creates a vulnerability that forces national security policy makers to prioritize the supply chain security of these technologies—including for semiconductors. Having to rely on an untrustworthy manufacturer of semiconductors itself creates a vulnerability.

- **Future technologies**

  Globally, analysts predict the semiconductor industry to continue its strong growth for years ahead due to emerging technologies coming online such as fifth generation wireless technologies (5G), autonomous vehicles, artificial intelligence (AI), and increased Internet of Things (IoT) applications.

---

43 Supra note 16.
46 Supra note 13.
Through its “Made in China 2025” plan, China seeks to dominate each of these high-tech areas and the next generation semiconductors which make them possible. Should China become a leading manufacturer of semiconductors, the future of our economic prosperity and national security would be reliant upon suppliers based in and governed by a commercial, military, political, and ethical rival.

- **Supply Chain Security**

Supply chain security is of utmost importance to the Pentagon. Semiconductors made specifically to military specifications (MilSpec) are manufactured at specialized foundries to ensure integrity. Semiconductors manufactured to MilSpec should not have malign or benign malware or counterfeit parts. Yet a single Senate Armed Services Committee investigation in 2012 found 1,800 cases of counterfeit electronic parts in defense equipment—each case not only presenting its own potential vulnerability, but also endangering the men and women serving the United States.

Should the domestic semiconductor industrial base collapse, the U.S. military and intelligence services could lose access to the critical, secure supply chains necessary to conduct safe and secure operations to protect the American people.

**POLICY RESPONSE TO THE THREAT**

**U.S. Response**

- **CFIUS/FIRRMA**

American Presidents used the Committee on Foreign Investment in the United States (CFIUS) five times to block foreign investment transactions since its inception in 1975, three of which impacted the semiconductor industry. In 2016, President Barack Obama used CFIUS to block the acquisition of Aixtron, a German semiconductor firm with significant U.S. assets, by Chinese firm Fujian Grand Chip Investment Fund. In 2017, President Donald Trump blocked acquisition of Lattice Semiconductor Corp. by Canyon Bridge Capital Partners, a Chinese investment fund. And in 2018, President Trump blocked acquisition of Qualcomm by Singapore-based Broadcom.

In 2018, Congress approved, and President Donald Trump signed into law, the first major reforms to CFIUS in a decade with adoption of the Foreign Investment Risk

---

47 Supra note 22.
Review Modernization Act (FIRRMA). The legislation targeted CFIUS review of national security risks in new areas including private equity investments and joint ventures acquiring sensitive technologies, including in the semiconductor industry.\(^{51}\)

- **Entity List**

In 2018, the United States Department of Commerce Bureau of Industry Security (BIS) added Chinese semiconductor company Fujian Jinhua Integrated Circuit Company, Ltd (Jinhua) to its Entity List in response to theft of intellectual property from U.S.-based Micron.\(^{52}\) The action forbids acquisition by Jinhua of U.S. components absent a license and led to the company ceasing operations the following year. Jinhua was utilizing U.S. DRAM technology for Chinese military use.\(^{53}\)

Last year, BIS added HiSilicon to the Entity List when it expanded Huawei’s listing to all global affiliates, including the fabless semiconductor giant based in Shenzhen.\(^{54}\)

- **Export Controls**

As part of the National Defense Authorization Act in 2018, Congress passed and the President signed into law the Export Control Reform Act. The ECRA sought to restrict exports to China of key foundational and emerging technologies, including semiconductors, citing a national security threat.\(^{55}\)

In August of 2020, BIS issued its long-awaited advanced notice of proposed rulemaking concerning foundational technologies from ECRA. The notice highlights that the export of semiconductor manufacturing equipment to indigenous military modernization efforts in China, Russia and Venezuela may pose a national security threat.\(^{56}\)

- **“Military End User” Licensure**

In September of 2020, the Commerce Department announced to companies doing business with SMIC that they would need to apply for “military end user” licenses—which had not previously been required. As these licenses are under review, American firms are not able to provide the tooling and other components necessary for

---


\(^{53}\) Id.


semiconductor production. As this measure is recently implemented, policymakers should continue to monitor how this addresses security threats and prepare for other warranted measures.

- Counterintelligence

Federal Bureau of Investigation (FBI) Director Chris Wray has said:

> The greatest long-term threat to our nation’s information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China.

80 percent of all economic espionage prosecutions brought by the U.S. Department of Justice are reported to involve cases that would benefit China.

In 2018, the United States Department of Justice unveiled a new China Initiative “to confront China’s malign behaviors and to protect U.S. technology.” The initiative specifies an effort “to better address supply chain threats, especially those impacting the telecommunications sector.”

- Domestic Production Incentives

In order to make domestic manufacturing and production of semiconductors more globally competitive, leading Members of Congress have authored legislation to provide significant tax incentives and research and development to support the industry. In the Senate, Senators John Cornyn and Mark Warner have introduced S. 3933, The CHIPS for America Act, which would provide $22 billion in financial incentives and R&D. Congressman Mike McCaul has introduced the House version.

Senators Tom Cotton and Chuck Schumer have introduced similar legislation called the American Foundries Act.

- Hong Kong

Following passage of a new national security law extending mainland governance and authority over the previously semi-autonomous region (SAR) of Hong Kong, the

---

Commerce Department extended export controls to China for key technologies, including semiconductors, to the Hong Kong SAR as well.\(^63\)

➢ International Push

The U.S. Department of State leads an inter-agency initiative to warn allies around the world on the inherent dangers of Chinese military-civil fusion and their growth in key dual-use technologies such as semiconductors. Dr. Chris Ford, Assistant Secretary in the Bureau of International Security and Nonproliferation said:

Military-civil fusion is a national-level Chinese effort led by Xi Jinping himself...to maximize its global geopolitical power by taking advantage of the “Revolution in Military Affairs” that Chinese officials envision arising out of modern advances in areas such as nuclear technology, aerospace, aviation, semiconductors, cloud computing, robotics, and “Big Data” processing.

On this topic earlier this year, Secretary of State Mike Pompeo said:

Even if the Chinese Communist Party gives assurances about your technology being confined to peaceful uses, you should know there is enormous risk to America’s national security.\(^64\)

Global Response

In 1996, the Wassenaar Arrangement was approved by 33 nations—since expanded to 40—as the first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies.\(^65\) Last year, the group updated the pact to include new language on semiconductors and semiconductor manufacturing equipment (SME).\(^66\)

➢ Netherlands

Media reports indicate that the Dutch government blocked a shipment of an advanced chip-making machine by Dutch SME maker ASML to China-based SMIC following high-level U.S. engagement.\(^67\)

---


Japan

Media reports have indicated that Japanese semiconductor firms, including Tokyo Electron, the number three global supplier of SME, would not sell to products to Chinese companies that end up on the BIS Entity List.68

Last year, media reports indicated that Japan was considering advanced technology exports controls like what the United States has promulgated focusing on the threat from China.69

India

In response to violent clashes along India’s border with China, killing dozens on both sides, India has banned 118 Chinese applications or apps.70 Media reports also indicate that India is moving to restrict Chinese telecommunications companies from building out future domestic telecommunications networks.71

This has led observers to note a change in Indian policy toward China when it comes to key technology issues perhaps forecasting key, additional technology import restrictions from China in the future.72

United Kingdom and the European Union

The United Kingdom and several major carriers in European Union countries including Belgium, France, Czech Republic, Poland, Italy, and Sweden have reportedly decided to not use Chinese telecommunications giants Huawei or ZTE to build out their 5G networks. Additionally, following additional U.S. export restrictions to Huawei, there are even serious discussions of an EU-wide de-facto ban.73 This indicates a leeriness of technology imports from China to the European continent.

---

71 Nikarika Sharma, “Indian telecom firms may take a hit if the government decides to ban Huawei.” Quartz, August 30, 2020. [https://amp.scroll.in/article/971562/indian-telecom-firms-may-take-a-hit-if-the-government-decides-to-ban-huawei](https://amp.scroll.in/article/971562/indian-telecom-firms-may-take-a-hit-if-the-government-decides-to-ban-huawei)
Taiwan

In response to increased aggression from China, Taiwan has taken a series of steps targeting mainland-based technology companies, including increased transparency of PRC-domiciled tech companies and a ban on certain PRC apps. This shows a strong concern from top Taiwanese government officials at the threat mainland technology policies pose to Taiwan’s sovereignty, security, and survival.

The largest semiconductor foundry in the world, Taiwan Semiconductor Manufacturing Company (TSMC), announced that it would not sell its high-end chips to Huawei or HiSilicon in accordance with U.S. regulatory restrictions.

South Korea

Though South Korea often gets caught in the middle of U.S.-China tech disputes, it has also sought technology independence from Beijing. Though Seoul prefers a less prescriptive path than Washington has taken, the result has aligned at times. As an example, South Korea decided to both boost its own domestic champions and limit reliance on China when it decided to contract Samsung and other domestic companies to build South Korea’s 5G network.

Media reports indicate that both Samsung and SK Hynix will cease supplying Huawei with high-end components including advanced chips. Samsung and LG Display are both reportedly planning to stop selling Huawei panels for premium smartphones as well.

RECOMMENDATIONS

- **Entity Listing**

  While the U.S. government has already taken steps to limit the transfer of sensitive technologies and components to Chinese counterparts, the efficacy of these measures should be evaluated by policymakers along with other measures that can be applied to ensure U.S. national security. Given the dual-use nature of semiconductors and the civil-military fusion in China, BIS should add SMIC, CXMT, YMTC and potentially other Chinese-domiciled semiconductor companies as

---

warranted to the Entity List. Sensitive U.S. components should not go to further the military technology of our primary geopolitical competitor. This action would likely have the tertiary impact of stopping key semiconductor imports from Japan and South Korea to leading Chinese industry players as well.

- **Export Controls**

BIS should conclude a swift, but thoughtful, interagency rulemaking for its export restrictions of foundational technologies to include high-end semiconductors and SME to the state-owned enterprises of adversarial nations like China and Russia.

- **Diplomatic Pressure**

The U.S. State Department should continue to lead the interagency on a global diplomatic effort to ensure allies understand the risks of using state-backed Chinese technology. The Department’s Clean Network Initiative programs should be expanded to include semiconductors.

- **Incent Domestic Production**

Domestic and allied production capacity should be a key consideration for policymakers as they consider policies affecting semiconductor supply chains and their security. To foster domestic capacity and continued U.S. innovation leadership, Congress should immediately approve and the President should sign into law the CHIPS for America Act or something similar to match the massive financial incentives China is pouring into its own state-backed industry, creating a national security threat to the U.S. and our allies.

- **Expand Defense Industrial Base to Semiconductor Production**

Expanding Defense Industrial Base authorities to semiconductor production would ensure U.S. or trusted allied semiconductor companies protect a Western or Western-allied manufacturing base. Utilizing the Industrial Base Fund and the Defense Production Act’s Title III financial tools, this would be done in a similar way to how the U.S. Defense Industrial Base protects ship, tank and airplane manufacturing lines, none of which function without high-end semiconductors.

- **Prepare for Retaliation**

Should the United States take the actions above, we certainly should prepare for retaliation by the Chinese government to related or potentially unrelated industries—including the detention or commencement of Chinese criminal proceedings against U.S. and allied citizens in China. The interdependence of U.S.-China technology industries and other commercial ties behoove the government to be aware of the impact that this could have on U.S. firms’ operations and revenue and citizens’ safety abroad, and it should plan accordingly.
CONCLUSION
Semiconductors are essential to much of the U.S. economic and national security of the present and future.

Though the United States does not need to act like China to beat China, we must not abandon the playing field entirely. A national strategy by our primary geopolitical competitor that includes state-backed research and development, state financing, a captured market of the world’s second largest economy, and state-sponsored IP theft cannot be met with wishful thinking.

Instead, to match the moment, the United States and our allies should take immediate action like that outlined above to secure the semiconductor and SME supply chain and prevent reliance on or infiltration by adversarial nations like China.