zenontech

Zen on Tech Newsletter

V16 - China's Options for Chip Security

2nd Sept 2023

Summary

Status of the Chip Choke. In October 2022, the U.S. ramped up sanctions on China's semiconductor industry, targeting advanced chips essential to AI development and pushing back China's technological aspirations. While SMIC, China's primary chip manufacturer, can produce moderately advanced chips, it risks regressing to 2003-level technology if completely cut off from U.S. advancements. While China is preparing their economy for potential US sanctions, we see clear evidence they are also preparing their industrial base for conflict.

China Expanding Production of Older Tech. In retaliation to the U.S. sanctions, China has fortified its older technology chip production. Beijing's $140 billion investment and SMIC's strategic refocus are evidence of this. While their emphasis remains on older technology chips, SMIC has witnessed significant growth, with its revenue soaring past $7 billion in 2022. SMIC's revenue is a mere tenth of TSMC's, while the difference in wafer shipments is only half: 7.1M wafers for SMIC compared to 15.2M for TSMC. This indicates a lower average selling price for SMIC and a predominance of older chip technology sales.

Expect US Response with Trade Duties. The U.S. should anticipate China's potential flooding of the market with legacy chips, a move that could shift the dynamics of the semiconductor industry. To counter this, the U.S. might employ proactive measures like antidumping/countervailing duties. However, considering that 70% of SMIC's revenue comes from China, we argue that any punitive duties would need to target final products using these chips to deter manufacturers from sourcing subsidized Chinese chips.

US Equipment Leaves China Vulnerable to Cyber Attacks. China's reliance on Western machinery interlaced with foreign control systems opens doors to potential cyber threats. Drawing parallels from events like the Stuxnet attack on Iran, China's infrastructure remains at risk. To curtail this vulnerability, China must innovate its industrial machinery, reducing its dependence on foreign systems.

China Expediting the US Free Chip Supply Chain. In the realm of semiconductor equipment manufacturing, Chinese companies face tremendous challenges in catching up. SMIC, while having a robust revenue stream and foundational machinery, is in a better position than its Chinese equipment maker counterpart, SMEE. As China treads the path towards 2030, the stakes are high: domestic manufacturing prowess is paramount to stave off potential production declines at the leading edge due to machinery degradation.

I don't currently think we can rule out SMEE launching a 14nm lithography machine by 2027. One pivotal marker to watch will be the slated release of their 28nm machine by the end of this year, which holds immense weight in mapping out China's semiconductor roadmap. Connecting these dots, we're reminded that the heart of this saga is intricately linked to China's desire for economic resilience amidst potential sanctions and Xi's strategic calculus in preparing for a Taiwan invasion by 2027. As the world closely watches the dance between technology and geopolitics, China's path in the semiconductor domain holds broader implications beyond just industry dynamics. The ebb and flow of their progress serve as a barometer for the nation's overarching objectives.

Contents

Principles of the Chip Choke

Delusions of Détente: Why America and China Will Be Enduring Rivals

In a geopolitical environment where technology is increasingly becoming the currency of power, China's phenomenal growth story appears to be hitting some significant roadblocks. The country faces a litany of internal challenges including massive debt, youth unemployment, and the looming threat of deflation. Xi Jinping's endeavors to turn this economic trajectory around bear implications not just for China but for the world at large. Measures needed to avert a debt-deflation spiral, assuage a restless middle class, modernize the military, enhance energy and food security, and pursue technological advancements, are monumental tasks that require vast fiscal programs. Furthermore, the possibility of taking more aggressive stances, such as a potential invasion of Taiwan, adds another layer of complexity.

Simultaneously, the West's two-decade-long policy of technology and knowledge transfer to China is coming to an abrupt stop. This backdrop sets the stage for the United States' "chip choke" strategy, which aims to cripple China's technological aspirations by refusing to contribute to its tech development. The strategy signals a pivot in Western policy towards China, moving from engagement and cooperation to containment and competition. At the core of this new approach are several key principles:

I. **"Mastery over core technological components leads to dominance in computation; and those who dominate computation rule the machinery world."** The United States holds a commanding position in this arena, a fact evidenced by the CHIP4 nations' alignment with the U.S. The heavy reliance of ASML—a pivotal company in the semiconductor industry—on U.S. technology underlines the gravity of potential divisions. Allies like Japan and Taiwan have quickly aligned their interests with the U.S., keenly aware of Beijing's growing influence. South Korea, also conscious of the existential challenges it faces, is negotiating but essentially siding with the U.S.
II. **"The U.S. is in a leadership position in crafting the primary machines which, in turn, produce subsequent generations of machinery."** The U.S. enjoys deep-rooted technical knowledge, especially regarding the vulnerabilities in the Chinese legacy fabrication plants. Such expertise can be leveraged for cyber operations aimed at hindering China's technological advancements. Companies like LAM, KLA, and AMAT provide software integral to these facilities, which are still years and vast sums of money away from achieving technological parity with the U.S.
III. **"Geopolitical interests will always overshadow commercial priorities."** For the orchestrators of the chip-choke strategy, economic consequences are secondary concerns. The U.S. perceives China as only the second significant existential threat in its history, the first being the British invasion of 1814. In this high-stakes geopolitical struggle, even major U.S. corporations like Apple, Tesla, and Nike are considered collateral damage.
IV. **"As China edges closer to technological independence and deviates from global standards, the U.S. will intensify and broaden its constraints."** Should China manage to circumvent current restrictions on AI chip and manufacturing technology, their success could alter the global power dynamics substantially. Such advances would, in turn, likely prompt the U.S. to escalate its technological restrictions on China, leading to a cyclical pattern of tensions between the two nations.

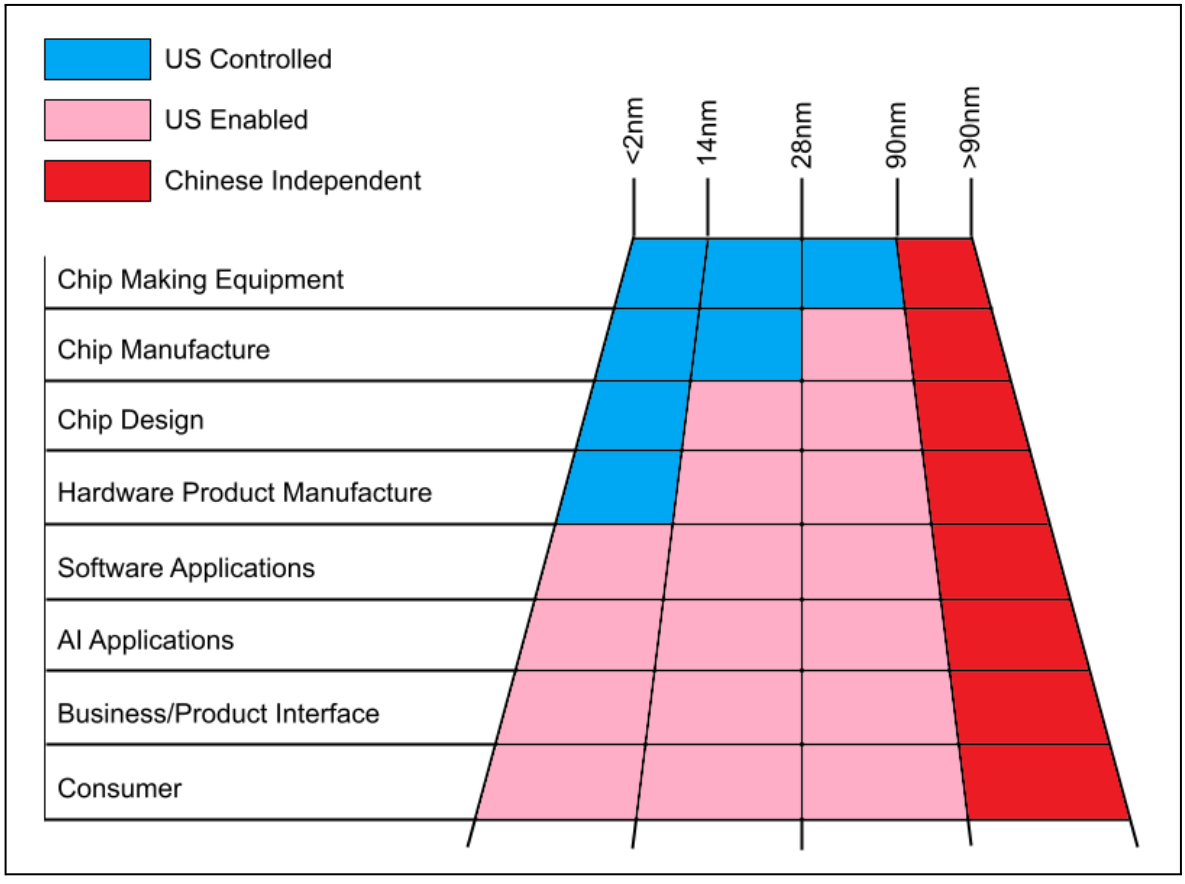
By embracing these principles, the U.S. seeks to proceed cautiously through the complex arena of technological globalization, always alert to the potential threats that may emerge from contributing to a rival's ascendancy. The "chip choke" initiative indicates that the Western strategy for containing China will increasingly involve what could be termed 'geo-tech warfare.' Consequently, China faces the challenge of going it alone in cutting-edge domains such as Quantum Information Systems, Semiconductors, and Artificial Intelligence. China's ability—or inability—to respond effectively will not only determine its own future but will also have ripple effects across the global stage.

Status of The Chip Choke

[Analysis: China's massive older chip tech buildup raises U.S. concern | Reuters]
[Chinese chipmakers urge Beijing to do more amid tension with U.S. - Nikkei Asia]
[Huawei Building Secret Chip Plants in China to Bypass US Sanctions, Group Warns - Bloomberg]

In October 2022, the U.S. increased restrictions on China's access to 16 nm chip making equipment or below, basic DRAM memory chips at 18nm or below or 128 layers or more for NAND, and prohibited accessing any of the most advanced AI processing chips. These restrictions, at the current level, primarily deal a blow to China's ambitions to emerge as an AI superpower and impede its capacity to develop domestic chips that are more advanced than 16nm.

Under the current sanctions, China's Semiconductor Manufacturing International Corporation (SMIC) may continue to mass-produce chips at a moderately advanced level of 28nm or even a low yield 7nm. However, should China lose access to all U.S. technology, its production capabilities could be severely curtailed, limited to 90nm chip production capability, taking it back to the technology levels of 2003. The graphic below shows where the current Chinese capability is at 90nm, where China needs to import US controlled technology and where the Chinese are building applications and processes on top of US controlled technology.



In response to the October sanctions Beijing allocated another $140 billion to subsidise domestic chip making equipment purchases. Additionally SMIC (China's foundry) has refocused on mature technology chips, announcing four new facilities in 2020. This expansion, according to analysts, could triple SMIC's output. We see the Chinese response to US sanctions as two fold 1) Expand production of older technology chips and 2) Expedite the development of a US free supply chain.

1. Expand Production of Older Technology Chips

Analysis: China's massive older chip tech buildup raises U.S. concern | Reuters
Chinese chipmakers urge Beijing to do more amid tension with U.S. - Nikkei Asia
China imports record amount of chipmaking equipment | Financial Times

Despite facing early hurdles, SMIC, backed by Beijing, has carved out a significant position in legacy chip technologies, as reflected in its 2022 revenue surpassing $7 billion (**Chart 1**). With U.S. export controls hampering the production of advanced chips, SMIC has pivoted its focus to traditional technology chips, launching four new facilities since 2020. Samuel Wang, a Gartner analyst, believes this growth could triple SMIC's output. Although SMIC's revenue is a mere tenth of TSMC's at over $70B annually, the difference in wafer shipments is only half: 7.1M wafers for SMIC compared to 15.2M for TSMC. This indicates a lower average selling price (ASP) for SMIC and a predominance of older chip technology sales.

Source: Financial Times

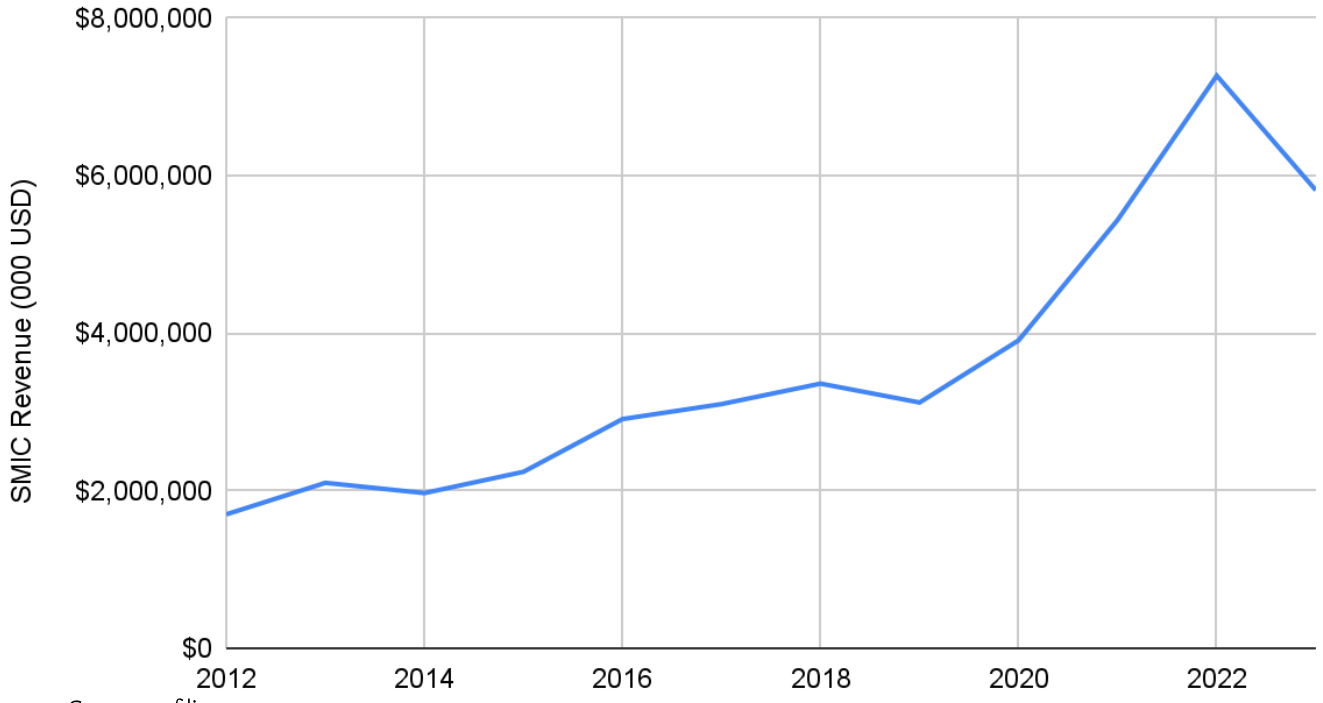
The apprehension around SMIC's emphasis on legacy chip technology is rooted in China's historical approach of flooding the market with affordable products, thereby edging out global rivals. Matt Pottinger, former Deputy National Security Advisor under the Trump administration, cautions, *"This tactic was employed with solar panels and 5G telecom gear, and could be replicated with legacy technology chips... Such a move would grant Beijing significant influence over nations and sectors, whether defense or commercial, reliant on 28 nanometer chips, which comprise a substantial segment of the chip market,"* Reuters.

The Semiconductor Industry Association (SIA) recently raised alarms about Huawei discreetly establishing a semiconductor production network throughout China. Such a clandestine venture could potentially enable Huawei to sidestep US sanctions, reinforcing China's tech aspirations. Having ventured into chip manufacturing just a year ago, Huawei has received an estimated $30 billion in support from the Chinese government and its Shenzhen base. As per SIA's findings, Huawei has taken over two facilities and is in the process of setting up at least three more. However, Huawei remains tight-lipped about these endeavors.

The worldwide semiconductor sector is witnessing a decline in device and semiconductor sales (Zen on Tech V15), with an exception for AI chips which are on the rise. Yet, chip manufacturing equipment exports remain robust in China (**Chart 2**), indicating a consistent, non-market driven, growth in chip production capacity.

China's significant capacity in legacy chip technology not only provides them with leverage in the global economy but also shields its economy from potential sanctions, especially in a scenario like a Taiwan conflict. However, this strategy also invites two forms of retaliation 1) Commercial weapons like broadening of the Chip Choke to older 28nm equipment and anti-dumping duties on Chinese chips and 2) Cyberattacks on US-based equipment and software operating in Chinese facilities..

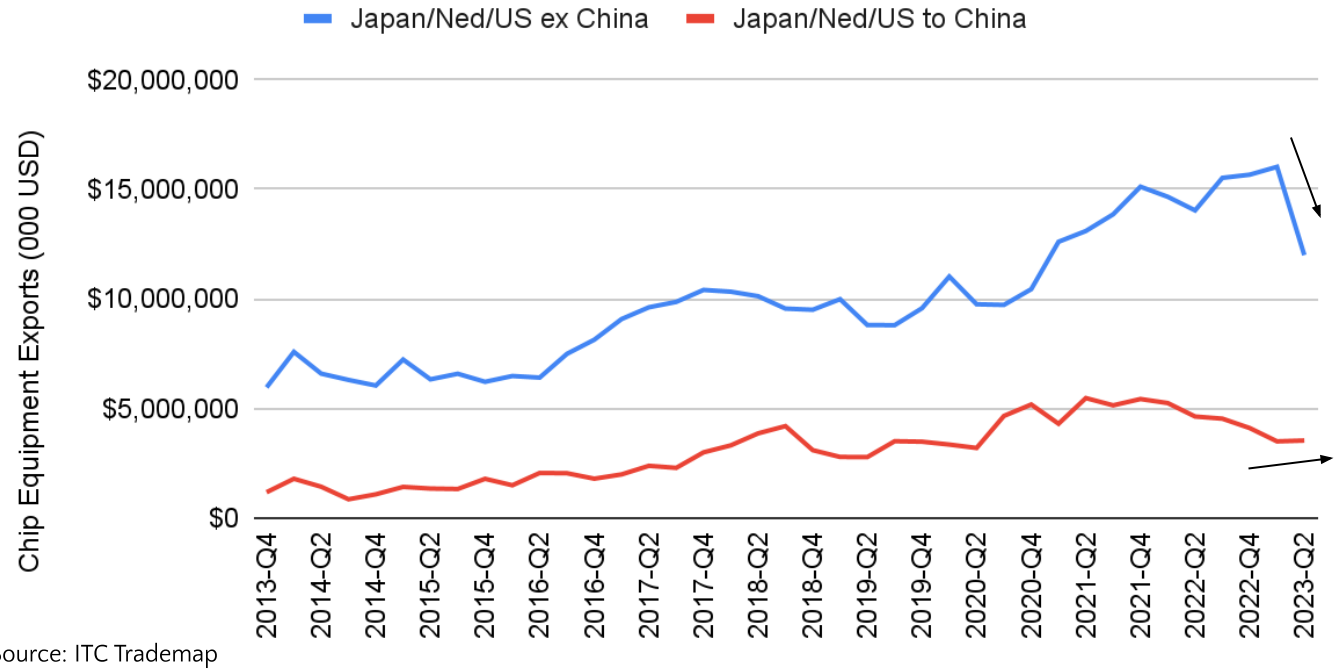
Chart 1, SMIC is Growing but Experiencing the 2023 Slowdown



Source: Company filings

Chart 2, Chip Equip Exports to China Stable, World Declines

Japan/Netherlands/USA Chip Equipment Exports



Source: ITC Trademap

Expect US to Respond With Trade Duties

The Silicon Triangle

China's strategy of subsidising capex for older chip technology can easily be construed as using state funds to dump below market products into the global market, provoking potential U.S. retaliation. A pivotal document, "*The Silicon Triangle*," penned by renowned thinkers and former government officials, already outlines a multi-faceted approach to this challenge.

The paper argues that the U.S. and its allies should leverage their dominance in the semiconductor supply chain as a form of economic deterrence against China's potential geopolitical aggressions. They propose that a dynamic approach to denying China technological superiority should focus on reciprocal actions and respect for a rules-based order. Given China's anticipated emphasis on mature nodes, they also recommend that the **U.S. should consider stricter export restrictions, potentially extending to the 28nm range**. The aim is to prevent China from gaining undue influence in this crucial segment of the global supply chain.

However, a lurking concern remains: even with rigorous U.S. export controls on equipment, China might inundate the global market with an abundance of legacy chips. This could see China capturing a significant portion of the semiconductor market, akin to its dominance in rare earths. This dominance could erode the U.S.'s manufacturing capability of these chips and dilute R&D profits for subsequent product generations. China could then channel profits from these legacy chips to counteract the effects of U.S. sanctions, further boosting its semiconductor research and education.

To mitigate these potential repercussions, the paper recommends the **U.S. to consider proactive measures, such as imposing antidumping/countervailing duties (AD/CVDs) on China-produced chips before any significant harm manifests**. Historically, AD/CVDs have been reactive measures, employed after domestic industries suffer, like the pattern in the steel industry. But given China's established industrial strategies, **preemptive imposition might be more apt**. If deemed insufficient, a more radical step could be the outright blocking of Chinese legacy semiconductor imports, nudging electronics manufacturers towards non-PRC chip sources or even prompting a manufacturing shift away from China.

While the U.S. could strategize to counteract the potential oversupply of older chips from SMIC, it's essential to consider the geographical distribution of SMIC's revenue streams. A significant 70% of SMIC's revenue originates from sales within China itself, followed by 20% from North America and a combined 10% from Europe and other parts of Asia. This distribution implies that even **if the U.S. were to impose duties on Chinese chip imports, the direct financial impact on SMIC would be confined to just a fifth of its total sales**. Furthermore, even if Europe, which historically tends to be more hesitant about such impositions, were to join the U.S. in this action, it would still only affect 30% of SMIC's sales. Thus, while such regulations might serve as a deterrent on paper, in practice, they would likely be a relatively toothless threat against SMIC's broader revenue landscape. Any duties would need to be targeted correctly. **Instead of just focusing on chips, the U.S. could impose AD/CVDs on final products that utilize these cheap chips. This would discourage manufacturers from using subsidized Chinese chips in their products.**

The Complexity of Tech Protectionism, Internet of Things Example

[China's Plan to Rule the World's Smart Devices, FCC Urged to Act]
[Mexico's Microchip Advantage: The Right Way to Shift the Semiconductor Supply Chain Away From China]

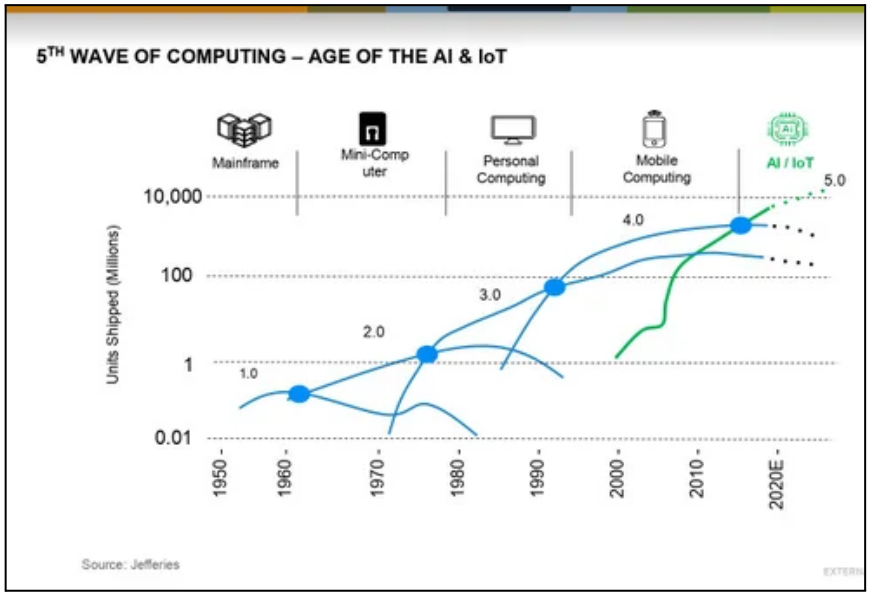
Chinese leaders have articulated the significance of technology, including the Internet of Things (IoT), in achieving their long-term strategic objectives. As early as 2009, IoT was identified by the Ministry of Industry and Information Technology as an "emerging strategic industry." Subsequent five-year plans—specifically, the 13th and 14th plans covering the years 2016 to 2025—also emphasized the role of IoT technology.

Quectel, a cellular module manufacturer and designated by the Beijing government in 2022 as a "national champion" in IoT, reported an annual operating revenue of just under $2 billion in 2022. According to Counterpoint Research, the company held 38.5% of the global market share for IoT modules based on volume. In total, Chinese companies constituted 77% of the global market by volume, including the large domestic market in China. Outside of China, these companies captured 53% of all sales by volume last year.

A notable impact of China's emphasis on legacy chips is the increasing likelihood that these Chinese-manufactured components will become ubiquitous in various "simple" products. These include Microcontroller Units (MCUs) used in distributed computing for vehicles, household appliances, industrial machinery, and Internet of Things (IoT) modules. At present, the market is primarily controlled by companies like Texas Instruments (TI), Analog Devices Inc. (ADI), STMicroelectronics (STM), and various Japanese manufacturers. These companies, often termed "catalog suppliers," generally do not specialize in cybersecurity. China aims to dominate this market segment through large-scale production and competitive pricing, facilitated by numerous Chinese semiconductor fabrication plants. The efficacy of using tariffs to counter this trend remains uncertain.

For a tangible example, consider a standard printed circuit board (PCB) used in an IoT device. This PCB collects sensor data, processes it, executes actions via actuators, and communicates with either a central controller or another cloud-based program. These boards generally contain a diverse range of components, such as legacy chips, motor drivers, WiFi MCUs, and low-end processor chips. These chips are often sourced from both Chinese and international companies and are assembled onto the PCB in China. Because these chips are scattered through devices, high end processing is often less important than minimising unit cost.

To disrupt this type of supply chain, the U.S. government would potentially target the $10 worth of components in a $45 PCB. In practical terms, a huge import duty or an outright ban would be required to significantly alter current procurement practices. Strategies focused on tinkering with percentage content or percentage of total value could prove complicated to implement. However, the supply chain could potentially shift to other Asian nations if their pricing is substantially cheaper. Vietnam in particular is gaining momentum in the electronics supply chain. Mexico is also capitalising on the emerging opportunity.



Source: NXP & Crank

US Equipment is Vulnerable to Cyber Attacks

NIST SPECIAL PUBLICATION 1800-10C – Protecting Industrial Control System Environments
Security Challenges and Requirements for Control Systems in the Semiconductor Manufacturing Sector
CSS Cyber Defence Report, Hotspot Analysis: Stuxnet

Various malware tools can be employed by nations to disrupt industrial control systems. Given potential tensions with the US and potential economic sanctions, China is likely fortifying its industries against such threats. Stuxnet, discovered in 2010, serves as an example. Though designed for widespread propagation, its main target was the centrifuges at Iran's Natanz uranium enrichment plant. In light of this technology's exposure, it's probable that Chinese cyber units are bracing for a similar tool to be reused.

How Stuxnet Works:

- **Propagation**: Stuxnet propagated via USB drives using a Windows vulnerability. Once the drive was connected to a Windows machine, Stuxnet would execute.
- **Seek and Infect**: After initial execution, it would seek out Siemens Step7 software, a tool used for programming industrial control systems (ICS) like those at Natanz.
- **Take Control**: Upon finding its specific target (specific configurations of Siemens PLCs), Stuxnet would intercept commands and replace them with malicious payloads, all while reporting to the control system that everything was operating normally.
- **Cause Damage**: For the centrifuges at Natanz, Stuxnet commanded them to rotate out of control, damaging the equipment, while the monitoring software indicated everything was functioning properly.

Implantation and Execution:

- Stuxnet exploited multiple zero-day vulnerabilities, which are previously unknown vulnerabilities to software manufacturers. This made it incredibly hard to detect and stop.
- The primary infection vector was USB drives. This was important because the Natanz facility was "air-gapped," meaning it wasn't connected to the internet. Physical access, possibly through unwitting insiders using infected USB drives, allowed Stuxnet to jump the air gap.
- After initial infection, Stuxnet propagated within the network, searching for its specific targets.

Could The Equipment Owner Have Protected Against It? In theory, yes, but in practice, it would have been challenging because; Stuxnet was highly sophisticated, using multiple zero-day vulnerabilities. It had valid digital signatures, making it appear as legitimate software. The targeted nature of the attack (specifically looking for Siemens Step7 software in a particular configuration) meant that generalised antivirus or intrusion detection systems would not easily pick up on its malicious activities. The use of USB drives as an infection vector bypassed the typical network-based protections.

"It bought us time. First, it was to get across from one administration to the next without having the issue blow up. And then it was to give Obama a little more time to come up with alternatives, through the sanctions," Cyber-attacks "bought us time" on Iran: U.S. sources | Reuters

Threat Modelling Industrial Control Systems

Lithography machines, such as those produced by ASML for semiconductor manufacturing, are specialised precision instruments. Due to their sensitive functions, they come with stringent security protocols. Typically, crucial machines like these in a semiconductor fab operate on isolated networks. Data transfers are executed via secure methods, bolstered by multiple layers of firewalls, intrusion detection systems, and additional safeguards against unauthorised access. Physical security at semiconductor fabs is equally rigorous, barring unauthorised personnel from these machines. However, the by far the largest cybersecurity risk in a chip fab would be if a major lithography machine producer, like ASML, worked with intelligence agencies to compromise equipment in specific nations. Potential scenarios include:

Points of Entry

1. **Sabotaging at the Manufacturing Stage**:
    a. **Hardware Tampering**: Components of the machine can be tampered with during manufacturing. This could include adding hidden circuits or modifying existing circuits to malfunction under specific conditions.
    b. **Firmware Alterations**: Modify the firmware so that under certain conditions (like after a specific number of operations or on a certain date) the machine malfunctions.
    c. **Embedded Malware**: Introduce malware into the machine's control software that can be activated remotely or under certain conditions.
2. **Supply Chain Interruption**:
    a. **Component Replacement**: As the machine passes through various checkpoints, third-party components could be replaced with compromised ones.
    b. **Software Updates**: Introduce vulnerabilities or backdoors through updates that come from the manufacturer or trusted vendors.
3. **Post-Installation Sabotage**:
    a. **Maintenance Vulnerabilities**: Use regular maintenance cycles as opportunities to introduce vulnerabilities. Technicians (unwittingly) could install compromised parts or software.
    b. **Remote Activation**: If the machines have any kind of network access, even if it's an isolated intranet, use this access to remotely trigger the sabotage mechanisms.
4. **Over-the-Air Updates**: If the machines are equipped to receive over-the-air updates, these can be used to push compromised software that includes the sabotage mechanisms.

Damage

1. **Induce destructive failure**: Like the centrifuges at Natanz, command machinery to operate out of control, damaging the equipment, while the monitoring software indicates all is functioning properly.
2. **Subtle Defects**: Instead of overtly damaging the production process, the machine could be made to produce minor defects that are hard to detect until much later, thus disrupting the supply chain and eroding trust in the affected country's semiconductor industry.
3. **Randomized Malfunctions**: The machine might malfunction unpredictably, making it hard to diagnose and leading to increased downtime and reduced output.
4. **Data Theft**: If the intent isn't just sabotage but also espionage, the compromised machine could be used to exfiltrate data on chip designs, intellectual property, or production techniques.

Possible Exit

1. **Plausible Deniability Mechanisms**: The sabotage could be designed in a way that mimics natural hardware failures or software bugs, making it hard to trace back to intentional sabotage.
2. **Self-erasing Malware**: As in the Stuxnet case, the malware could be designed to delete itself after it has achieved its purpose, making post-incident forensics more challenging.

Incident Response for the Chinese Fab

1. **Immediate Isolation**: Disconnect the affected machinery from all networks, both internal and external. This prevents potential malware from communicating with external servers or spreading within the internal network.
2. **Backup and Data Preservation**: Back up all logs, configurations, and data from the machine. This will assist in forensic analysis and might help restore the system to a functional state more quickly.
3. **Hardware Examination**: Physically inspect the machinery for any unauthorised devices or tampered components. This includes checking for any anomalies in components, wiring, or ports.
4. **Firmware and Software Analysis**: Compare the machine's firmware and software with known clean versions to detect any alterations or anomalies.
5. **Forensic Analysis**: A detailed forensic analysis can reveal how the machine was compromised, what the malicious payload does, and how it operates.
6. **Restoration (may not be possible)**: Once the nature and extent of the compromise have been understood, restore the machine to a clean state. This might involve; replacing compromised hardware components, reinstalling firmware and software from clean sources and restoring configurations from known good backups.

Preventative Measures for the Chinese Fab

To safeguard machinery, ensure that pivotal systems remain isolated from external networks and maintain collaborations with only verified vendors, implementing robust encryption in supply chain communications. Regularly validate hardware and firmware against secure versions and enhance physical security by restricting machinery access. Adopt the "zero trust" principle, updating systems frequently while ensuring a protective process for these updates. Emphasize segmented networks, rigorous staff training, and equipment tests in isolated environments. Deploy advanced monitoring tools, continuously verifying software and firmware integrity while observing machinery behavior for inconsistencies.

Conclusions

Stuxnet, a highly sophisticated malware, was stealthily introduced into the Iranian nuclear program's machinery through an external USB device. This malware manipulated Iran's centrifuges at Natanz, causing them to spin uncontrollably and resulting in significant equipment damage. Such cyber threats leverage zero-day vulnerabilities, which are initially undetected and potent but eventually identified and patched in an ongoing cyber cat-and-mouse game. In the wake of revelations like the Snowden leaks and the exposure of Stuxnet, China is undoubtedly bolstering its cyber defenses.

However, the extensive use of Western machinery integrated with foreign industrial control systems in China's infrastructure poses a plethora of potential cyber vulnerabilities. Some of these threat gateways resist complete mitigation, leaving an ever-present risk. Considering the possibility of warfare or economic sanctions, this elevates the threat landscape to a dauntingly high risk level. It's conceivable that US intelligence might discover a zero-day flaw that could instigate fires, cause permanent equipment damage, or embed stealthy trojans within device patterns, leading to later malfunctions.

While it might seem improbable to find a singular "off switch" to paralyze China's burgeoning semiconductor industry, a combination of US trade embargoes, pressure on supply chains, and malware attacks targeting industrial control systems can significantly hinder its progress. The diverse avenues for potential sabotage of Western equipment in China underline the imperative for China to innovate and produce its own industrial machinery, thus reducing its vulnerability to external cyber threats.

2. Expedite The US Free Chip Supply Chain

Analysis: China's chip sector needs more than state money to dull impact of US restrictions | Reuters
China chipmaking tech execs urge greater supply chain self-sufficiency - Nikkei Asia
Deep Dive: SMEE and China's Attempt to Replace ASML Tools | EqualOcean
China to receive first homegrown lithography machine this year
Huawei to restart 5G mobile chip output as early as this year - Nikkei Asia

China is investing heavily in its semiconductor sector to offset October U.S. export bans, committing $140 billion for domestic equipment as of December 2022, benefiting firms like Shanghai Micro Electronics Equipment (SMEE), China's sole semiconductor lithography expert.

SMEE primarily caters to local foundries rather than collaborating with top-tier chip manufacturers like TSMC or Samsung. This restricted interaction hampers their progress, as few of their R&D innovations make it to mass production. In the semiconductor industry, companies often form strong partnerships with clients to push the boundaries of technological advancement together. However, Chinese firms, like SMEE, encounter challenges in this arena. For instance, SMEE began without any profound knowledge in lithography and primarily relied on studying second-hand equipment and publicly available patents. While they have managed to produce 90 nm machines, they still fall short when compared to industry leaders like ASML. Consequently, there's an absence of effective strategies that would allow Chinese equipment companies to reach the forefront of technological innovation.

There are a litany of people in the Chinese chip industry expressing concern for their ongoing development.

- *"Even if we could have built the machines, we wouldn't have known how to service and maintain them," the engineer said.*
- *"We knew what it takes to do that, but we were limited by the equipment's design capability. Our U.S. rival had already solved that," the staffer said."*
- *"When the sanctions came out, all the American companies followed," an engineer at a Chinese memory chipmaker told Reuters.*
- *"When we bought our equipment, we used to get customer service. Now we can't even get that because of the sanctions.""*

Analysis: China's chip sector needs more than state money to dull impact of US restrictions | Reuters

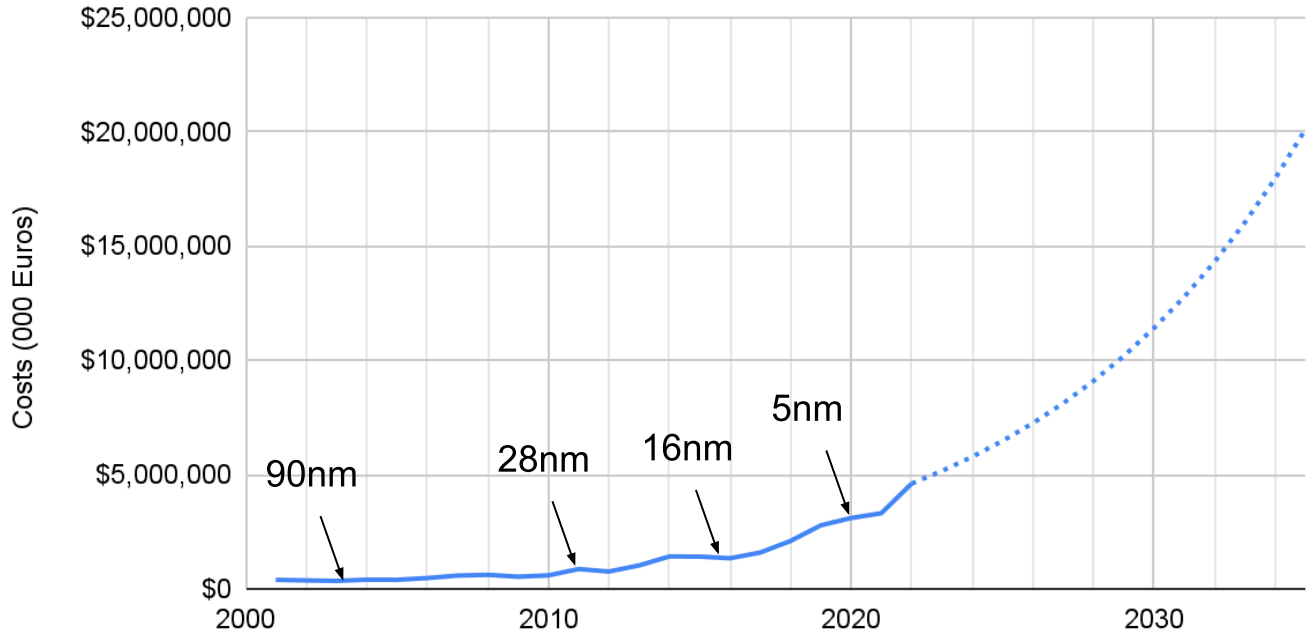
China's path to the 5nm domestic supply chain

Considering ASML's trajectory from 90nm tools in 2003 to 2nm by 2023 over a 20-year span, SMEE's projection, based on their 90nm release in 2017, hints at a 2nm achievement by 2037. Given this lengthy duration, it's clear the CCP will seek ways to expedite this progression. We've examined multiple factors influencing the two primary dimensions—time and investment—for SMEE to parallel ASML's advancements.

This thought experiment emphasises solely on R&D/CAPEX costs, omitting elements like R&D subsidies, revenue, and operational finances. The majority of these costs will be to SMEE but some will be externalised to the broader supply chain but we have not differentiated the two as it will come from government subsidies at the end of the day. We discern two developmental phases: 1) A massive influx of governmental capital addressing technical hurdles and 2) Self-sustenance wherein the firm must generate its own income. These are very rough numbers but they provide a lens for looking at Chinese technological progress. Please challenge our assumptions; we would love to make this more accurate.

ASML took 8 years to progress from 90nm to 28nm, another 9 years to progress from 28nm to 5nm and another 3 years to reach 2nm (**Chart 3**). Over that period of time, ASML's R&D and CAPEX spend was US $30B.

Chart 3, ASML Took $30B and 20 Years to Develop 2nm EUV



Source: Company filings

Analysis of SMEE replicating ASML's Development

Cost adjustments:

Deduction: -20% (Reverse engineering capability)

Addition: +10% (Cyber risk mitigation)
+30% (Shortage of experienced semiconductor engineers)
+30% (Potential corruption and inefficiencies)
+40% (Expedited development)

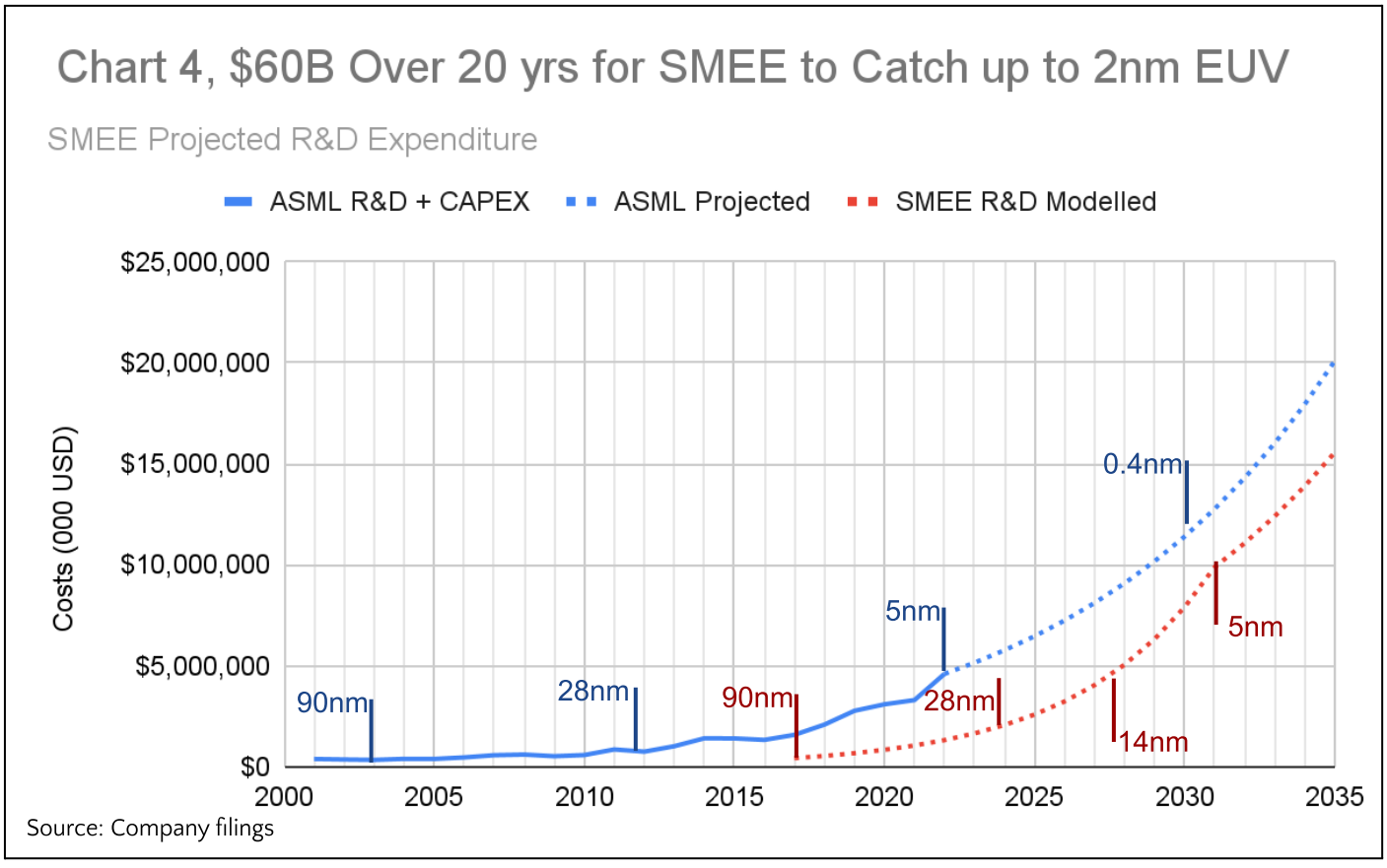
Resulting in an approximated 90% increased costs compared to ASML's R&D budget, making SMEE's projection US $60B.

Time adjustments:

Deduction: -30% (Unlimited budget)
-30% (Reverse engineering capability)
-10% (Reduced market/sales diversions)
-10% (Tightly-knit customer feedback)
-10% (Closeness to affordable suppliers)
-10% (Intense developmental urgency)

Addition: +40% (Building out the supply chain)
+30% (Potential inefficiencies and corruption)
+30% (Shortage of experienced semiconductor engineers)

Summing up to roughly no time-savings compared to ASML. Hence, SMEE's projection from 90nm to 28nm is approximately 8 years which indicates that they will be aiming to have their 28nm machine market ready within a year. Their current publicly stated goal is to deliver a 28nm machine in 2023. According to our analysis SMEE will be aiming for 5-7nm by around 2030-2033. Concurrently, ASML/TSMC may reach 0.4nm/500 picometres by 2030 (**Chart 4**).



Source: Company filings

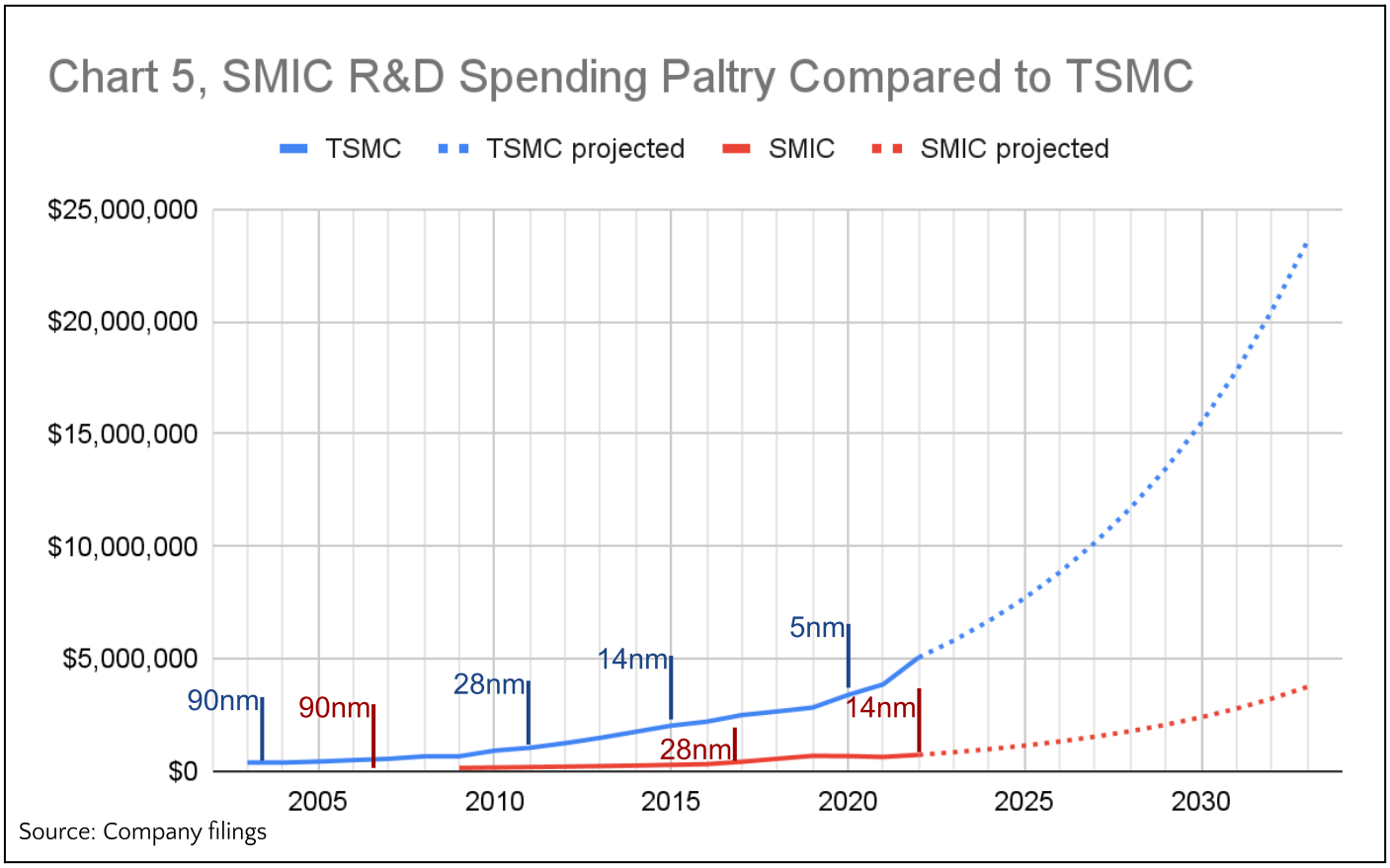
Historical Comparison: SMIC and TSMC

During the golden age of Chinese IP theft, SMIC managed to trail TSMC's technology at a far lower cost than what we have modelled for SMEE (**Chart 5**). We believe there are two main reasons that the challenge will be greater for SMEE.

Ties between China and Taiwan: SMIC's ability to trail TSMC at a lower R&D cost primarily benefited from the proximity and human ties between China, Taiwan, and Korea. This geographical and cultural closeness facilitated, among other things, the transfer of intellectual property, potentially through less than official means. Additionally, the main companies in this space are based in the Netherlands and Japan, creating a geographic and cultural distance that wasn't as pronounced in SMIC's case with TSMC.

Chip Making Equipment is more Complex than Fabs: The semiconductor capital equipment sector (like ASML's specialty) differs fundamentally from fabs (like SMIC). The intricacies, precision, and technicalities involved in lithography machines, for instance, make them extremely complex and challenging to reverse engineer or imitate. ASML's EUV machines are at the pinnacle of modern engineering and the result of decades of research. While reverse engineering can reveal how a device works, the tacit knowledge, intricate details, and fine-tuning that go into ASML's machinery will not be as easily replicable. The deductions factor in the advantages of reverse engineering, budget, and proximity to suppliers. However, the difficulty in ironing out inefficiencies, training a skilled workforce, and maintaining consistent quality across the board will be gargantuan.

While SMEE could leverage some of the benefits that aided SMIC in the past, the challenge of catching up to ASML is of a different magnitude. The complexity and precision of semiconductor equipment make it an entirely different ball game from fabs. It's plausible that with significant investment and the right partnerships, SMEE could close the gap over time. However, it will require a strategic and sustained effort, and even with a favorable cost and time analysis, achieving parity with industry leaders like ASML will be a monumental task.



Source: Company filings

Conclusions

In the fiercely competitive world of semiconductor equipment manufacturing, Chinese manufacturers are grappling with profound challenges. Within an open market system, the path to catching up seems nearly insurmountable, given the substantial R&D barriers. For instance, SMEE, would require an investment of approximately US$60B to develop 5nm lithography machines by decade's end, a cost that's hard to justify without a clear revenue generation strategy.

Yet, the scenario for China's leading fab, SMIC, is not as dire. Operating on a solid revenue stream, SMIC possesses lithography machines that can serve a decade if well-maintained. While acquiring advanced 7nm or 14nm machines is no longer an option, they have a solid foundation for initiating production. Conversely, SMEE is facing a ticking clock; they have a mere half-decade to match up to 14nm technology. Failing this, SMIC's frontline production might be compromised due to machinery wear and tear.

This looming predicament showcases China's imminent vulnerability. Until 2030, the nation will lean heavily on foreign chip-making equipment for anything up to 14nm, a situation that becomes a prime target for cyberattacks, particularly in geopolitical conflicts. By the next decade, China will find itself at a pivotal juncture: either achieve domestic manufacturing prowess with chip making equipment or grapple with a decline in production capacity due to machinery deterioration.

As of now, I estimate a balanced 50% likelihood of SMEE rolling out a 14nm lithography machine by 2027. A key predictor to gauge this trajectory will be their forthcoming 28nm machine, anticipated by year-end after several postponements. With the broader picture in view, it's vital to recognize the Chinese Communist Party's strategic goals for 2027, which pivot on economic resilience against sanctions and strategic moves regarding Taiwan.