The Shadow Supply Chain: Cybersecurity Risks in AI Hardware and Semiconductor Manufacturing

Mehak Farooq (student), Mehjabin Majid (advisor)

1. University of Punjab
2. Marine Academy of Technology & Environmental Science

Corresponding Author Emails:

1. mehakfarooq950@gmail.com
2. itsmehjabin@gmail.com

Abstract

Semiconductors are the backbone of the modern technology providing power to smartphones and artificial intelligence systems and defense applications. The global supply chain that sustains semiconductor [i]production is highly complex, as it relies on a complex network of distributors, suppliers from all around the world. This is a complex network with many threads that need to work together. However, much of their supply is concentrated in specific regions like Taiwan and South Korea creating significant vulnerabilities. Cyber threats, geopolitical tensions and disruptions in production or delivery can not only delay supply but also expose sensitive information to theft. Such disruptions have far reaching consequences, driving up costs for companies and posing serious risks to both economic security and national security.

The rise of unofficial supply network often called as the shadow ***supply chain*** poses a growing challenge to semiconductor industry. These networks operate outside the formal recognition of the companies often emerging due to cost pressure, that drives firms to seek cheaper, informal and unauthorized providers. Lack of visibility beyond tier suppliers makes it easy for shadow vendors to enter unnoticed. The rise of shadow supply chain is possessing serious to national security and international stability beyond technical concerns because this can cause the sanction addition of tampered chips into the critical systems, which compromises reliability and security. To reduce these potential risks this study emphasizes the need for advanced verification mechanisms such as block chain enabled systems and strengthened international cooperation.

Introduction

The modern era is the era of technology and microchips are the fuel of it, these are capable of doing multiple tasks from smart phones to advanced Ai systems, and to satellites in civil and military technology, all need microchips to operate. The designs of these chips are made in USA and the fabrication is done in Taiwan (Patel, 2024). According to world economic forum global supply chain is at risk. Due to the emergence of shadow supply chain and unauthorized access of hardware that added a layer of risk to the national security of a state. The shadow supply chain means that some chips slip into the market without the formal approval because they look similar to the original one and are passed unnoticed through regular checks.

For instance, in United States 1700 memory components from unauthorized suppliers have been used and falsely marketed as new, once the compromised parts were identified and removed the resulting expenses exceeded $4 million. Similarly in 2020 U.S air force raised a serious concern when defective transistors and semiconductors contributed to a failure of parachute system leading to fatal malfunction (Kulkarni, 2021). These cases highlight that how these vulnerabilities compromise the reliability safety and security beyond these risks it also causes serious economic consequences.

This research fills a critical gap in the discourse on the semiconductor security. It highlights the geopolitical importance of semiconductors and associated risks in concentrated regions like Taiwan and South Korea. The research focus is on shadow supply chain, an informal network that allows tampered chips to slip into the global markets (Solingen, 2025).

This gap is significant because most policy focus official supply chains and they neglect or overlook, how shadow networks bypass sanctions as explained in the cases of China and Russia. This short research paper exposes the hidden dimensions and also contributes on purposing solutions such as Block chain enabled verification systems, golden chip databases to ensure authenticity of the chips. It also emphasizes the need for international cooperation and policy harmonization, considering semiconductors as strategic global good rather an economic commodity. My research bridges the gap between technical risks and strategic concerns, making it valuable for policy makers, industry leaders and strategists.

Discussion

Case studies

Semiconductors have become strategic instrument in global politics, their role is beyond traditional economic good. This shift is well illustrated in recent US-China rivalry over Ai race. Washington has imposed restrictions on advanced chips to contain Chinas progress in artificial intelligence, statistics reveal that between May and July 2025 alone, more than USD 1 billion worth of banned NVIDIA AI chips were smuggled into China through third-party intermediaries. Intelligence reports indicate that 39 newly established Chinese AI centers collectively acquired around 115,000 restricted NVIDIA GPUs. In response, the United States has begun installing trackers within chip shipments to monitor distribution and detect potential diversions (Haider & Hanif, 2025).

In Russia-Ukraine war Moscow received the toughest technology despite sanctions, these sanctions aimed to weaken Russia military capabilities by cutting supply of certain components. Despite these restrictions Russia was able to circumvent restrictions with the help of the shadow supply chain. This informal network enabled countries to continue sourcing chips necessary for both civilian industries and its defense sector. For example, between March 2022 and June 2025 a company in Belarus delivered more than 130-million-dollar western made chips to Russia including parts used for military and AI advancement. This case highlights that how sanctioned state can exploit network of allied partners in order to maintain the flow of restricted goods. This shows systematic weakness in current enforcement mechanisms and intelligence driven approaches to block the misuse of global semiconductor supply chains. Russia's primary semiconductor lifeline is China recent trade data reveal that nearly 89 percent of semiconductors of Russia originate from China. The cost of these imports has surged dramatically, rising from $1,411 per kilogram in 2021 to $2,730 per kilogram in 2023. Despite this steep increase, Moscow has shown little concern for economic inefficiency, underscoring the strategic priority it places on maintaining chip inflows. To bypass sanctions Russia has established pipeline network through Hong Kong, turkey the UAE and the other intermediatory hubs where weak or irregular export practices enable western technology to slip through. This has allowed Russia missile system, drones and radar technologies to remain dependent on western designed chips. Investigations of components recovered from downed Russian weapons in Ukraine confirm the presence of chips traced back to Western manufacturers, illustrating how easily dual-use technology infiltrates global markets. Russia's case shows that export controls are not enough when states rely on supply chains operating in grey zone of global trade. This highlights urgent need for international cooperation, need for improvement in transparency and intelligence driven disruption of shadow networks to ensure that sanctions retain their intended strategic effect

Strategic implications for security and resilience

a. Detection and verification

Stronger Detection and verification mechanisms can be helpful in addressing the risks of shadow supply chain. Recent studies highlight the potential of combining blockchain enabled systems with physically unclonable functions **PUFs** which serve as unique fingerprint for individual chips (Ahmadi-Assalemi, Al-Khateeb, Epiphaniou, Cosson, Jahankhani, & Pillai, 2019). this combination makes it possible that each chip can be authenticated throughout their lifecycle reducing the risk of counterfeit or compromised components entering circulation.

In addition, the establishment of "**golden chip**" databases repositories that store trusted reference profiles of chips, including characteristics such as power consumption and performance behavior can provide rapid verification. Such systems make it possible to quickly detect anomalies or tampered hardware before they infiltrate critical defense, communication, or infrastructure system

b. Diversification of Production

A second principal recommendation is to minimize the world's dependence on a single geographic area specifically Taiwan for semiconductor production. With TSMC holding more than two-thirds of global foundry market share, any hiccup, be it due to cyberattacks or geopolitical tensions, could have disastrous ripple effects. To counteract this exposure, there is an ongoing attempt to increase production capacity elsewhere. TSMC's upcoming fabrication facilities in the United States, along with comparable investments in Japan, South Korea, and the European Union, are tangible moves to diversify production. Such geographic diversification does not remove risk completely, but it lowers the chances that one event could disable global chip supply.

c. Sturdy Cyber Defense

In addition to supply chain visibility, firms also need to secure their cyber defenses to safeguard semiconductor manufacturing itself (Pakes & Pitts, 2023). Conventional security practices are not adequate in this industry. Since chip making entails sophisticated physical processes, intruders who breach these environments might embed nearly imperceptible but ruinous faults within hardware. Thus, companies must use digital defenses in tandem with hardware-centered audits, ongoing supplier screening, and in-real-time monitoring of manufacturing environments. By taking cybersecurity practices into the operational and physical layers of semiconductor production, organizations are able to develop resilience against digital as well as cyber-physical attacks.

Policy and cooperation

United international policy and cooperation is required to address this problem, that is because single companies or nations on their own cannot accomplish it. Semiconductors traverse various borders frequently using diverse standards of rules.to prevent this division exploited by different networks nations need to harmonize the standards sharing information and developing clear mechanisms throughout the industry, because semiconductors are now a direct security threat to national security, international community must consider them as strategic global good that needs collaborative governance measures to balance the economic competitiveness with collective cooperation (Bhattacharjee & Chakraborty, 2025). This will generate perilous effects, primarily in defense. Because of shadow supply chains, countries can avoid export controls and employ it for military as well as AI advancement. For instance, the US utilized microchips of firms such as Texas instruments that were brought to Russia for military use. The US applied rigorous restrictions on advanced node chips in order to prevent China from acquiring key technologies. China retaliated by imposing restrictions on key minerals such as gallium required in semiconductor manufacturing. Russia was able to obtain microelectronics such as the US produced chins from sophisticated supply chains regardless of third-party firms as well as nations such as China, which consequently destabilizes the system reliability.

Conclusion

Thus, the rise of shadow supply chain poses severe risks to economic stability, technological reliability and national security. Counterfeit and unauthorized chips infiltrate critical systems undermining trust and exposing vulnerabilities. Case studies of China and Russia show how easily restrictions can be bypassed through opaque network. Stronger detection mechanisms, diversification of production, and robust cyber defenses are essential. Ultimately, only coordinated international cooperation can safeguard the semiconductor supply chain against these growing threats.

References

Patel, D. (2024). *Semiconductor supply chain security: Identifying US-China chip war impacts & Europe's strategies* (Bachelor's thesis, Metropolia University of Applied Sciences). Theseus. https://www.theseus.fi/bitstream/handle/10024/883750/Patel_Dhruvalkumar.pdf?sequence=2

Kulkarni, A., & Xu, C. (2021). A deep learning approach in optical inspection to detect hidden hardware trojans and secure cybersecurity in electronics manufacturing supply chains. *Frontiers in Mechanical Engineering, 7*, Article 709924. https://doi.org/10.3389/fmech.2021.709924

Etel Solingen (2025) “Global value chains in a brave new world of geopolitics”, Journal of Political Power, 18:1, 112-124, DOI: 10.1080/2158379X.2024.2447249

Haider, B., Hanif, S., & Fida, Z. (2025). The Geo-Political Implications of the US-China AI and Tech Rivalry. *Global Social Sciences Review, X(II)*, 45-54. https://doi.org/10.31703/gssr.2025(X-II).04

Ahmadi-Assalemi, G., Al-Khateeb, H. M., Epiphaniou, G., Cosson, J., Jahankhani, H., & Pillai, P. (2019, January). Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. In *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)* (pp. 1–9). IEEE.

Pakes, A., & Pitts, F. H. (2023). *Cybersecuronomics: Cybersecurity & Labour's modern industrial strategy*. Progressive Britain. https://ore.exeter.ac.uk/repository/handle/10871/134208

Bhattacharjee, A. & Chakraborty, S. (2025). Global Supply Chain Networks: Roles of Global

Partnerships and Governance in Supply Chain Performance. In P. Channaganu & R. Yanamandra (Eds.), *Global Partnerships and Governance of Supply Chain Systems* (pp. 189-222). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3693-6987-6.ch007