Chip War and the Battle for Technological Sovereignty: A Hybrid Warfare Perspective

Description

Editorâ??s Note: this article is being republished with the permission of Small Wars Journal as part of a republishing arrangement between IWI and SWJ. The original article was published on 04.16.2025 and is available here.

SWJ Logo Tall

Chris Millerâ??s *Chip War: The Fight for the Worldâ??s Most Critical Technology* provides an in-depth analysis of the semiconductor industryâ??s pivotal role in global power dynamics. Integrating the insights from the Hybrid Center of Excellenceâ??s Comprehensive Resilience Ecosystem (CORE) framework, we can assess how recent developments among key industry players align with or diverge from Millerâ??s predictions, particularly concerning hybrid threats and systemic vulnerabilities.

Semiconductors as a Hybrid Warfare Battleground

In the CORE framework, hybrid threats are defined as multi-domain strategies that exploit systemic vulnerabilities to undermine democratic institutions, economic stability, and national security. Millerâ??s analysis of the global semiconductor supply chain perfectly aligns with this concept. The worldâ??s reliance on a handful of key playersâ??such as Taiwanâ??s TSMC, the U.S.â??s Intel, and the Netherlandsâ?? ASMLâ??exposes critical infrastructure to potential disruption from adversarial state and non-state actors.

One of the bookâ??s key takeaways is that microchip supply chains are not merely an economic concern but a central pillar of national security. The U.S.-China rivalry over semiconductor dominance exemplifies how economic interdependencies can be weaponized. This is a classic case of economic

hybrid warfare, where states use trade restrictions, technological embargoes, and cyber espionage to exert pressure on adversaries. The U.S. export bans on advanced chips and fabrication equipment to China, coupled with Chinaâ??s retaliatory measures, fit within the broader spectrum of hybrid threats outlined in CORE.

Miller highlighted the strategic vulnerabilities stemming from the concentration of semiconductor manufacturing in specific regions, notably East Asia. The CORE framework emphasizes the importance of diversifying critical infrastructure to mitigate hybrid threats. Recent geopolitical tensions have underscored these concerns. For instance, the U.S. has implemented export controls to limit Chinaâ??s access to advanced chipmaking technologies, aiming to maintain its technological edge. This move aligns with Millerâ??s prediction of increasing bifurcation between Chinese and non-Chinese spheres in the semiconductor industry.

Strategic Vulnerabilities and Systemic Risk

The *Chip War* narrative underscores one of the core principles of the resilience ecosystem model: the need to secure critical infrastructure and mitigate cascading failures. The book highlights how the concentration of chip manufacturing in Taiwan represents a massive single point of failure in global supply chains. Taiwanâ??s geopolitical vulnerability is not just a regional issue but a systemic risk to global economies and security.

From a hybrid warfare perspective, this is an Achillesâ?? heel that can be exploited through disinformation campaigns, economic coercion, or even military actions. The CORE framework warns of the dangers of over-reliance on foreign technological capabilities, particularly in sectors as critical as semiconductors. Chinaâ??s push for self-sufficiency through its â??Made in China 2025â?• initiative is a direct response to this vulnerability, illustrating a strategic shift in hybrid resilience.

Miller predicted a bifurcation between the Chinese and non-Chinese spheres in the semiconductor industry. China has been actively pursuing self-sufficiency in chip production, investing heavily in domestic manufacturing capabilities. However, recent reports indicate that Chinaâ??s purchases of chipmaking equipment are expected to decline in 2025, suggesting challenges in its quest for self-reliance.

Cyber Threats and the Weaponization of Technology

Miller also explores how semiconductor technology is integral to cybersecurity and cyber warfare. Advanced AI-driven cyber operations, deepfake disinformation campaigns, and digital espionage all rely on cutting-edge chips. The book details how U.S. and Chinese intelligence agencies compete for semiconductor supremacy, a key enabler of both defensive and offensive cyber capabilities.

The CORE framework highlights cyber resilience as a crucial component of national security. The semiconductor industryâ??s entanglement in cyber warfare underscores the necessity of protecting supply chains from espionage, intellectual property theft, and sabotage. The book warns that semiconductor fabrication facilities are prime targets for cyberattacks, and securing these assets should be a top priority for policymakers.

Miller discussed the relentless pace of innovation in semiconductor technology. Recent data supports this, with global semiconductor sales increasing by 19.1% in 2024 and projections indicating continued double-digit growth in 2025. Companies are making substantial investments to stay at the forefront of technological advancements. For example, NXP Semiconductors has entered into an agreement to acquire Kinara, Inc., aiming to enhance its capabilities in high-performance, energy-efficient, and programmable discrete neural processing units.

Lessons for Resilience Against Hybrid Threats

Millerâ??s analysis offers several strategic lessons that align with the CORE modelâ??s resilience-building approach:

1. **Diversification of Supply Chains** â?? The extreme concentration of semiconductor production in Taiwan and South Korea creates strategic vulnerabilities. As the CORE framework suggests, nations must develop redundant and resilient infrastructure to mitigate the impact of external threats.
2. **Human Capital Development** â?? A critical issue highlighted by Miller is the shortage of skilled labor in semiconductor manufacturing. This challenge persists, with companies like TSMC facing delays in their U.S. projects due to difficulties in finding qualified personnel. Efforts to address this include training programs and international collaborations to develop a skilled workforce capable of supporting the industryâ??s growth.
3. **Technological Sovereignty** â?? Dependence on foreign semiconductor technology can be exploited through hybrid threats. The U.S. CHIPS Act and the European Unionâ??s push for

semiconductor autonomy align with the CORE principle of reducing systemic dependencies.

4. **Investment in Domestic Innovation** â?? Resilience against hybrid threats requires a proactive approach to innovation. Miller highlights the importance of public-private partnerships in semiconductor research and development, a key strategy in mitigating technological vulnerabilities.
5. **Cybersecurity in Critical Infrastructure** â?? Protecting semiconductor manufacturing facilities from cyberattacks is a national security imperative. The book underscores the need for robust cyber defenses in safeguarding technological assets.
6. **Geopolitical Risk Management** â?? The book reinforces the idea that national security is no longer just about military power but also economic and technological resilience. Hybrid warfare strategies targeting semiconductor supply chains must be countered through coordinated policy responses.

Conclusion

Chris Millerâ??s *Chip War* is not just a history of the semiconductor industryâ??it is a warning about the future of global security. Through the lens of the CORE framework, the book serves as a case study in how hybrid threats exploit technological dependencies. Semiconductor dominance is not just about economic growth; it is a key battlefield in irregular warfare, where economic leverage, cyber capabilities, and geopolitical strategy intersect.

As states race to secure their semiconductor industries, the lessons from *Chip War* are clear: resilience against hybrid threats requires systemic thinking, proactive policymaking, and a recognition that technological power is inseparable from national security. For policymakers and security professionals, Millerâ??s book is an essential read in understanding how the microchip is now a frontline weapon in global competition.

Through the lens of the CORE framework, itâ??s evident that the semiconductor industry continues to navigate complex challenges and opportunities. Many of Millerâ??s predictions have materialized, particularly regarding geopolitical tensions and the push for supply chain diversification. Ongoing investments in technology and workforce development are crucial to building resilience against hybrid threats and ensuring the industryâ??s sustainable growth.

Disclaimer: The views expressed here are his own and not that of any part of the US Government.

Robert Redding

Dr. Robert Redding (Colonel, ret. US Army) is a national security practitioner with global experience in security cooperation and diplomacy. His military service include operational assignments in conventional and special operations units as well as at the US embassies in Tel Aviv and Ljubljana.

Date Created
2025/05/28