AI-Designed Chips and the National Security Imperative

By Brett J. Hamilton
CEO, Hamilton Microelectronics Consulting
https://www.hamilton-micro.tech/
www.linkedin.com/in/brett-hamilton-6a5764202

Soon, the most powerful weapons systems in the world could be powered by microchips designed by artificial intelligence—chips so complex, current tools and workflows cannot converge on a solution for how they work.

That future is no longer hypothetical. It is unfolding now.

AI is rapidly transforming how integrated circuits (ICs)—the tiny brains inside our fighter jets, satellites, missile defense systems, and secure communications—are designed. Traditionally, engineers carefully iterate on each step in the logic design and physical implementation of a chip. Today, artificial intelligence-based EDA tools and workflows are becoming capable of designing entire circuits on their own, pulling from vast libraries of reusable design blocks or creating new ones in real time.

This innovation is astonishing. It also represents a significant national security risk when in the wrong hands!

The Black Box at the Heart of National Defense

Modern defense systems are only as trustworthy as the hardware they run on. The problem is, we are relinquishing full control—or even full visibility—into that hardware. Most Department of Defense (DoD) systems now rely on **commercial-off-the-shelf (COTS)** components—hardware that is often designed by global teams, fabricated, and packaged overseas, far beyond U.S. oversight.

As chip designs grow more intricate, and AI increasingly takes over their creation, our ability to verify their integrity—let alone their security—declines sharply. If we cannot inspect and understand the hardware we use, how do we know it hasn't been compromised? The uncomfortable answer is: we don't.

Hidden backdoors, surveillance functions, or reliability compromises could be inserted into chips without detection. And AI-generated designs, while efficient, are often so complex and abstracted that no human could easily identify such malicious code—if they can at all.

A Race We Can't Afford to Lose

We are witnessing the emergence of an AI arms race—one in which foreign adversaries could use our reliance on AI and foreign chip manufacturing against us. They may already be doing so.

The challenge goes beyond espionage. It strikes at the core of strategic deterrence. If we can no longer trust our own microelectronics for modernization, we may be forced to revert to older, legacy systems that are secure but outdated—putting our forces at a serious disadvantage on the battlefield.

Worse still is the sci-fi scenario in which AI eventually designs chips that subtly assert control over the systems they're embedded in. This isn't science fiction anymore—technologists and scientists including the late Stephen Hawking and Steve Wozniak have raised red flags about the unchecked growth of AI in high-stakes domains.

Solutions Exist—But We Must Act

The good news is that solutions are within reach—if we act now.

We must develop **independent verification tools** that can cross-check AI-generated chip designs before they reach the manufacturing stage. These tools must be capable of identifying unintended or malicious functionality and ensuring design integrity throughout the production lifecycle.

Congress can help by funding research into **secure AI-aided chip design tools**, promoting **onshore manufacturing** and **secure packaging**, and establishing **design-to-fabrication traceability standards** for defense electronics.

Public-private partnerships will also be key. American companies and universities are already doing cutting-edge work in this space—but they need support, collaboration, and national-level coordination.

This Is a National Security Imperative

We can no longer afford to treat microchip design as a backroom engineering detail. It is a **frontline issue in 21st-century national security**. Every missile, drone, or secure network we field relies on microelectronics that must be trustworthy by design.

In the era of AI-designed hardware, trust is no longer automatic. It must be built—intentionally, transparently, and with urgency.

About the author:
Brett J. Hamilton is the founder of Hamilton Microelectronics Consulting and a senior advisor on secure microelectronics for defense and aerospace systems.