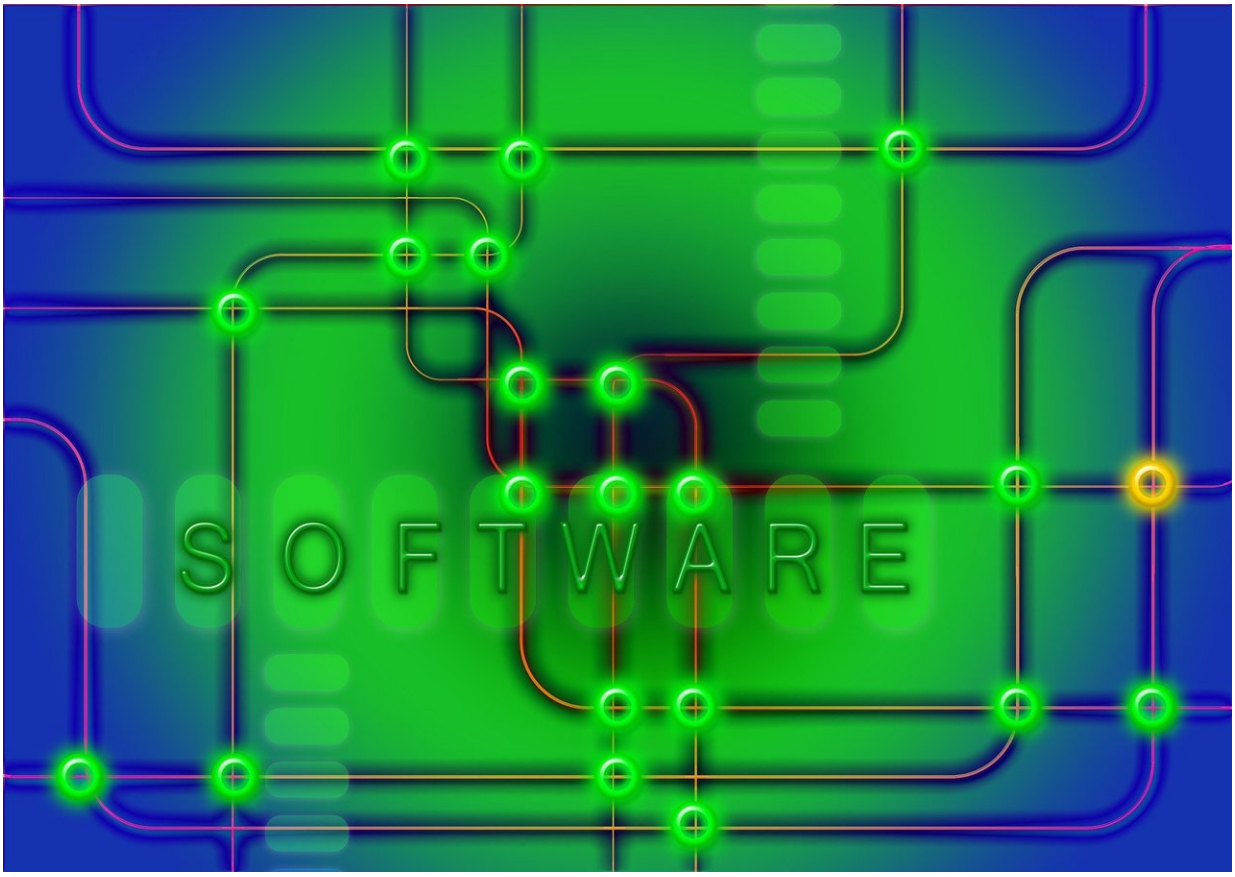
Microchip security continues to confound Pentagon

April 9 2021, by John M. Donnelly



Credit: CC0 Public Domain

Nearly nine years ago, the Senate Armed Services Committee reported the results of an investigation of counterfeit electronic parts in the U.S.

military. The year-long probe found fully 1 million bogus parts, including components for several types of combat aircraft.

"Our report outlines how this flood of counterfeit parts, overwhelmingly from China, threatens national security, the safety of our troops and American jobs," said Sen. Carl Levin, the Michigan Democrat who chaired the panel at the time.

Worries have only grown since then that technology that was made or modified in China, including everything from computer chips to servers, can be not just counterfeit but also malicious if it carries spyware.

The Pentagon has taken steps since then to try to shore up its vulnerability to questionable parts. When it comes to semiconductors, the building blocks of digital products, U.S. defense and intelligence agencies are still grappling with how to ensure those parts are not just available when needed—but also secure.

China's role in the Pentagon supply chain has grown considerably, and China's share of the Defense Department semiconductor market, in particular, grew from 7 percent to 13 percent from 2010 to 2019, according to a report last year from Govini, a research firm.

American companies still lead the world in semiconductor designs. But President Joe Biden and a bipartisan chorus in Congress have expressed concern about the American economy's reliance for its semiconductor manufacturing on not just China, which now builds more chips for the world than America, but more so on companies in two nations friendly to the United States: Taiwan and South Korea.

The upshot is that nearly 90 percent of U.S. computer chip manufacturing needs comes from East Asia.

In 2021, an ongoing shortage of computer chips, triggered by pandemic-induced disruptions in markets, has led to U.S. factory closures and job losses, and this has focused politicians' minds on the U.S. dependence on overseas chip makers.

On March 31, Biden proposed $50 billion in semiconductor manufacturing and research subsidies, and leading lawmakers from both parties have his support.

But having a "secure" chip supply should mean not just assured access to the products but also should inspire confidence that the products are trustworthy and reliable, leading analysts say. That is nowhere more important than when the chips are used in military and intelligence equipment.

"We all understand this is important not only to our economy but also to our national security, because these cutting-edge, high-end semiconductors operate on everything from the F-35 fifth-generation stealth-fighter plane to our cell phones," said Sen. John Cornyn, R-Texas, after a Feb. 24 White House meeting on proposals for subsidizing domestic chip makers.

Culture change

Congress is pushing the Pentagon to find ways to ensure the security of its computer chips. The fiscal 2020 NDAA—the defense authorization law—directed the Defense Department to develop a system for monitoring the trustworthiness of its semiconductors and to implement it by 2023.

In January, the Pentagon quietly delivered to Congress a draft report laying out an initial, broad take on what such a system would look like, defense officials said.

Now those officials say they are trying to put meat on the bones of that plan—to craft a detailed path forward for "trusted and assured microelectronics."

The focus, they say, is how they will better monitor the reliability and security of semiconductors from commercial production lines, regardless of where they are located.

At issue are chips that can be used in a variety of defense applications—from the most sophisticated and specialized systems, such as classified satellites, to the more pedestrian semiconductors on assets such as Army trucks.

Buying commercial chips for highly sensitive systems is a cultural shift for the Pentagon that does not come easy, said Mark Lewis, a former top Pentagon official who now runs the Emerging Technologies Institute at the National Defense Industrial Association.

"It's fine to say, 'I've got a brand new chip, it's commercial, I'm buying off the shelf,'" Lewis said. "But how do I have the confidence that anything I buy commercial is going to work in my DoD system? It comes back to the point that the systems of the Department of Defense have to work."

Shifting approaches

About 17 years ago, the Pentagon created a so-called Trusted Foundry program to obtain chips that absolutely had to be secure from a couple of dedicated Defense Department fabrication facilities, or fabs, in the United States.

That effort has grown since then to include not just a few builders of chips but also companies that do testing, packaging and more—some 78

industry participants as of last year.

This program covers only about 2 percent of the chips the military buys, a small but important portion that includes chips for highly secret programs or those, for example, that need to be hardened to survive radiation in space or in a nuclear war.

Defense Department officials recognize that their market comprises only about 1 percent of the ever-growing global demand for semiconductors. As a result, the Pentagon cannot have much influence over how semiconductor technology is developed, nor is it economically sustainable for any fab to focus on expensive, secure production facilities just for the Pentagon.

"This presents two potential risks," the Congressional Research Service said in a recent report, "a reduced ability to influence technology development and a loss of unique access to state-of-the-art technologies."

Kim Herrington, acting principal director of the Defense secretary's industrial policy office, said in an interview that the Defense Department is "in a potentially unhealthy way over-reliant on foreign sources, but we don't have a big enough demand to do anything about it in terms of driving the market."

Christine Michienzi, chief technology officer in the industrial policy office, said in an interview that the department does not have enough demand "to sustain a dedicated foundry or even a dedicated line within a foundry."

Nonetheless, Congress believes some sort of specialized defense capabilities will still be needed going forward. In fact, the fiscal 2021 NDAA law authorizes the Pentagon to provide incentives for the

creation of private-sector consortiums that can develop and produce "measurably secure" microelectronics for vital missions such as defense, intelligence and critical infrastructure. The funding for that program and other semiconductor initiatives—both those contained in that most recent NDAA and those proposed by Biden this week—has yet to be enacted.

Don't trust and verify

Increasingly, though, Congress and the department want to move away from the trusted foundry model and instead devise ways to ensure that the chips themselves, wherever they come from, are certified in tests to be trustworthy and reliable.

Chips made by American companies on U.S. soil are preferable, but those are few and far between nowadays. And being American is no guarantee of being trustworthy, just as being foreign does not necessarily make a supplier suspicious, experts said.

The focus of the new approach is less on who makes the product and more on whether it meets defined standards—measures that are still being developed, said Victoria Coleman, the Air Force's chief scientist, in an interview.

"Would you buy a stroller to put your baby in that had not been tested if someone told you all the workers in the factory are very good Americans who try their best and no foreigner ever crossed the threshold?" Coleman said. "Process doesn't buy you anything."

The Pentagon is trying to find out how industry does it. The department is writing into the contracts it signs with chip designers and foundries a requirement to provide access to corporate data on assessing chip reliability, according to Brett Hamilton, deputy principal director of the

Pentagon's microelectronics office, which is part of the office of the undersecretary for research and engineering.

"If you think about it, if the chip doesn't operate properly, whether it's an innocent mistake somebody made, or whether it's something that was done purposefully, many of the same techniques and mechanisms can be used to detect that," Hamilton said. "That data provides a solid foundation on which to apply additional mitigations based on the specific threat scenario and operational use of the chip."

The other major prong in the effort is to employ the latest methods of manufacturing chips, which include ways to construct them in pieces so that the various builders do not know the products' final purpose and so the U.S. military can tailor the semiconductors with security features.

Recently, software flaws are most often the route hackers take into key systems. But government and industry officials worry, Hamilton said, that to the degree those vulnerabilities get addressed, malevolent actors will soon try to use hardware as the preferred assault mode.

"Our attacker is going to take the path of least resistance," he said.