The U.S. Defense Department's New Thinking on Microelectronics Security

By Dr. Lisa Porter

Microelectronics are fundamental to essentially every technology and capability in the Defense Department and more broadly in the commercial world. While there are numerous examples that support this assertion, one emerging application worth highlighting is the next generation of cellular network technology, commonly referred to as '5G'. Ultimately, 5G is all about ubiquitous connectivity, which means a transition to fully distributed computation, communications, and data curation and management. Highly networked heterogeneous sensors, edge computing, machine learning algorithms implemented on all kinds of platforms, dynamic spectrum sharing, and so forth – all of these 5G elements will depend upon the ability of the microelectronics industry to continue to produce even higher bandwidths and better energy efficiencies, with smaller footprints, as well as increased flexibility and functionality.

However, we cannot just chase performance. While Moore's Law has guided the industry's focus on performance for decades, we must now focus on security as well. The Internet of Things (IoT), 5G, and distributed interconnected devices in general, present significant security challenges that encompass software, firmware and hardware.

When we consider all of the attack vectors and vulnerabilities that we will need to address, all the way down the stack, and all throughout our supply chains, the problem can seem insurmountable. If we are not careful, we can fool ourselves into thinking that the best approach to this complex, globally intertwined world is to try to wall ourselves off, to create perfectly secure and isolated systems. Instead, we must shift our thinking about trust and security.

There are lessons to be learned from the cybersecurity community. For well over a decade, many were focused on trying to build perfectly secure cyber systems, which led to significant investments in perimeter-defense approaches, leaving networks and data that were “inside the perimeter” extremely vulnerable.

Fortunately, today, the computer network security community has largely embraced an approach that is commonly referred to as a “zero trust” model. In zero trust, one does not assume that a network, or individuals using a network, are trustworthy simply because they reside behind a “wall.” Rather, one assumes that every network is already compromised and that individuals within walls will make mistakes, and one develops security architectures accordingly.

Similarly, when it comes to microelectronics, we in the U.S. Government need to move away from failed approaches of locking down everything within physically protected enclaves while the rest of the world accelerates its capabilities without our participation. While trusted foundries at trailing nodes fulfill an important Defense Department need, the trusted-foundry-model is outdated and cannot provide us the access we need to the most advanced manufacturing capabilities. The 5-to-10-fold increase in performance going from 130 nm to 10 nm simply cannot be discounted in our systems for which size, weight, power, and cost are always key drivers. Furthermore, IoT applications, and machine-learning inference engines at the edge, will demand leading-edge technology to meet very stringent performance and power requirements. We in the Defense Department cannot afford to be shut out of all of those capabilities, and more. In other words, taking an approach to security that binds us to old technology does not really make us secure at all.

In order to avail ourselves of leading-edge technology, we must develop data-driven security techniques and protocols that are complimentary to advanced commercial design and manufacturing processes so that we can protect our designs and ensure that what we procure functions exactly as intended. And no matter what size the node and what type of foundry we are using, data—not perimeters —must be the ultimate arbiter of the trust that we assign to the electronics that we build.

A lot of work lies ahead of us to effectively adopt a holistic, “zero-trust” approach to security in microelectronics. Data collection and analysis methods must be developed and applied along the entire lifecycle, in a manner that does not introduce significant throughput impact or prohibitive cost penalties, in order to effectively counter security threats that include malicious insertion, fraudulent products, theft of intellectual property (IP), and quality and reliability failures. Such methods could include scalable environments for design assurance, obscuration and marking methods, and multiple verification and validation tools and techniques.

In response to the challenge that lies before us, the Defense Department has begun a new initiative called Microelectronics Innovation for National Security and Economic Competitiveness, or MINSEC. It is focused on four key objectives:

(1) Ensuring that the U.S. Government has access to state-of-the-art design, assembly, packaging, and test capabilities

(2) Developing data-driven quantifiable assurance methods that will enable us to fabricate export-controlled designs within standard commercial domestic facilities

(3) Investing in niche capabilities that are essential to our mission, to include radiation-hardened electronics, and specialized RF and electro-optical chips;

(4) Working with academia to increase the throughput of electronics talent in our education pipeline.

The Defense Department believes that our desire to protect our design IP and to have confidence in what we procure, regardless of the source, are goals that are well aligned with the needs of the commercial customers– such as the automotive, telecom, medical, and industrial markets – that will be driving the electronics industry into the future. These companies are becoming acutely aware of the security threats that they face, and of the liabilities that those threats pose to their businesses. Therefore, we think it makes sense to collaboratively develop security standards and methodologies across the industry, and we want to work with the private sector to do that through MINSEC and other collaborations.

Finally, it is worth commenting briefly about the state of the United States' global competitive posture. It is important that we take the long view and play to our strengths, which include our culture of innovation, our free market principles, our entrepreneurial spirit, and the rule of law. Greatness is achieved not by cheating or stealing, or by focusing on holding others back, but rather by continually pushing to excel, running faster, and simply being better than everyone else. While we clearly need to take punitive action against IP theft, the day no one is trying to steal from us is the day that we should truly be concerned. In the world of microelectronics, the United States and our partners and allies currently enjoy a dominant position of global technological strength, and we in the Defense Department are committed to support the industry as it strives to continue to be the best.

Dr. Lisa Porter is the Deputy Under Secretary of Defense for Research and Engineering. Together with the Undersecretary of Defense for Research and Engineering, she is responsible for the research, development, and prototyping activities across the Defense Department enterprise. In addition, they oversee the activities of the Defense Advanced Research Projects Agency (DARPA), the Missile Defense Agency, the Strategic Capabilities Office, Defense Innovation Unit, the DoD Laboratory and Engineering Center enterprise, and Under Secretariat staff focused on developing advanced technology and capability for the U.S. military.