Raising the Bar for Software in National Security and Defense.

When COVID-19 forced much of the Department of Defense (DoD) workforce to shift to remote work environments, the largest and most complex agency in the federal government faced a real challenge. The monolithic organization, for which security is a key mission, had to figure out how to move operations out of traditional military environments and into people's homes. Former Principal Deputy Director of National Intelligence Sue Gordon and Vice President of Wireless Services at Google and Defense Innovation Board Member Milo Medin joined Rebellion Defense cofounder and CEO Chris Lynch for a panel discussion focused on this issue and other ideas about how leaders and managers should think about technology and software for defense and national security.

In the not-too-distant days before the cloud, businesses ran their data and systems in local offices, a situation that would have presented monumental challenges for operationalizing a mostly remote workforce. "One of the really interesting things that COVID has taught us is the power of the cloud," Medin said. "COVID has shown actually how people can flex." With data in the cloud, people not only can access that data, but they can do it in a secure way.

Even before COVID, Gordon noted, advantage and threat in the national security realm were a function of data—using or denying access to create advantage. Gordon indicated that the next step for the national security community, now that cloud computing has facilitated the ability to work together outside the office, is to figure out how to make that work even more secure. Sharing data, she said, is one of the greatest challenges that demands attention. Gordon said not only must DoD be able to operate in the way it did before COVID-19, but also it must be able to operate in the way it needs to at a distance. "All this data that each of us produce, can that data work together?"

Medin and Gordon both underscored the need to rethink network security moving forward. "The model of security is really about zero-trust," Medin said. As end-users' position on a network "becomes a signal and not a key," a zero-trust approach supports sharing of data and collaboration in a way that traditional security measures employed by DoD cannot.

Gordon agreed, "You've got to say goodbye to the moat. The moat model is just not the right model. It probably wasn't the right model before, but it certainly is not the one now."

In dealing with data, Gordon said operators need to make sure the data they produce has a pedigree to it. "We are not going to any longer be able to know everything about where our data are going, so

partnerships@rebelliondefense.com

Small Business • DUNS 100653409 • CAGE 8DAY4 •
NAICS Codes 511210, 518210, 541511, 541715

you have to be able to trust that they are going to transit in a reasonable fashion." She also warned that people need to be critical thinkers again.

So how can the technology industry create highly effective software for national security? Gordon says the capacity among U.S. companies is immense and expanding, but developers need to approach technology innovation with a particular idea in mind: "Oh, you wanted it to work?!" To ensure that ideas and capabilities can be optimally leveraged by DoD, Gordon suggested developers need to create software that can operate in the government system and that it can scale. If the government cannot figure out how to use a solution, implementation will be minimal at best. For example, if security is an issue, then software must be developed with authority to operate in mind.

As for what the government can do to ensure it has access to the best quality software, Gordon emphasized, "Quit over-specifying in RFPs." When the government over-specifies, new ideas can't possibly take hold, she explained.

Medin noted that another issue the government faces is its approach to using commercial software systems. "The government a lot of times thinks of software systems like hardware, and they are not the same. Software doesn't age well." Despite an apparent commitment to use commercial technology over DoD-developed solutions, the government tends to ignore the shelf life of these products and run systems that are obsolete. In doing so, Medin explained, "You are isolating yourself from that innovation and the capability that comes along."

The solution to this issue, Medin said, is to stop optimizing for cost and instead optimize for time. There is a view that change is dangerous, and the status quo is safer. "My friends in the Air Force and fighter community have a saying that 'speed is life,' and speed in the software community is life."

Gordon noted that technology can help reduce risk, and that if developers can show how the risk is accounted for differently, solutions can be adopted more quickly.

Lynch concluded the discussion by asking a critical question: What can be done to bridge the gap between Silicon Valley and the Pentagon?

Medin suggested that the government needs to focus more on problems because engineers are captivated by solving problems. The United States no longer has the advantage of being the sole holder of technology, so the focus must be on how the technology is created and integrated. "Being able to talk about the problem, being able to work with the Valley, and being able to take those people and technology and iterate rapidly is gonna be the key for the United States remaining competitive and furthering our lead in many of these areas."

The government, Gordon said, has big problems it is trying to solve, coupled with reasonably deep pockets and long horizons. She recommends this situation be leveraged by investing more in foundational R&D. "We have left the private sector to carry so much of the weight."

Gordon said the government needs to share more about the threats it faces, so companies interested in partnering with the government can better understand where to invest. "The purpose of the government, the energy of the private sector—those two have to come together to get some good global leadership thinking."