Department of Defense

The New Cyber Normal

Tom Michelli
Deputy Chief Information Officer
Department of Defense

We're refining the metrics to make them more meaningful and relevant to how it adds lethality and efficiency to the Department.

At Defense, **Tom Michelli** uses its Cyber Scorecard to measure the success of its security efforts.

DoD has tens of millions of endpoints, tens of millions of users and keeping track of how we're securing all those systems and people is a daunting task, Mr. Michelli explained.

"So we started with the people and the processes. We had weekly data calls with the components focusing on how we can work together on how we're meeting those tasks with measures and metrics. "

Through this effort, DoD began automating the process. "We went from almost all data calls to adding simple data feeds," Mr. Michelli noted.

"Now we have about 12 different systems; we are automatically updating the system; we're refining the metrics to make them more meaningful and relevant to how it adds lethality and efficiency to the Department."

Based on this success, DoD is about to embark on Cyber Scorecard. 2.0 that focuses on people and processes.

"We're working the DIUX (Defense Innovation Unit Experimental) that taps into Silicon Valley," he said. "We are looking how we can make this more real time, with more feeds, more artificial intelligence machine learning to have a real-time risk assessment and cyber resiliency."

The cyber scorecard also showed DoD some of the reasons why progress was slow certain places — one of which was multiple operating systems, Mr. Michelli added.

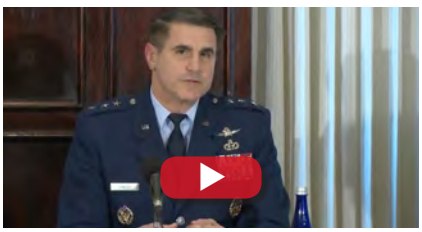
"We knew if we were on one operating system platform, we could do so much goodness, so much faster. We made the decision to go to Windows 10 which required the partnership, the leadership of the department both from the mission leaders, the financial leaders to the CIOs to make that happen."

US Air Force

Spy vs. Spy: Shrinking the 'OODA Loop'

LTG Bradford Shwedo
Chief Information Officer
US Air Force

In dogfighting, there's an old adage that 'speed is life'; and that is never truer than in cyber. We need to operate at the speed of cyber.



Air Force CIO **LTG Bradford Shwedo** did not mince words describing the cyber threat America faces.

"In dogfighting, there's an old adage that 'speed is life'; and that is never truer than in cyber. We need to operate at the speed of cyber. We are literally in a 'spy vs spy' game every day with bad guys wiggling windows, trying to get in our back doors."

To operate at the speed of cyber, the Air Force challenge was maintaining and managing an aging infrastructure with 600,000 endpoints worldwide, where every major command used to have its own infrastructure.

"Now we have rolled all those infrastructures up with a program called Automated Remediation and Asset Discovery — ARAD."

With ARAD, the Air Force rapidly found, patched and remediated assets very quickly; what used to take weeks, months is now being done rapidly.

"So fundamentally it has been very, very successful", LTG Shwedo noted. "Having the capability where you can push 'enter' and then all of a sudden having it all patched, that's when you start getting in the 'spy vs spy'.

"Going back to a dogfight, one of our goals is to shrink the enemies "**OODA Loop**". The phrase OODA Loop refers to the decision cycle of observe, orient, decide, and act, developed by military strategist and Air Force Colonel John Boyd. Boyd applied the concept to the combat operations process, often at the strategic level in military operations.

"In dogfighting speed wins, whoever shrinks that 'OODA Loop' down the fastest wins," LTG Shwedo explained.

"Then if you're really good you start introducing errors into the other side's 'OODA Loop', making theirs long and lethargic. When we talk about operating at the speed of cyber, we are talking about getting in the back doors of the bad guys and get it incorporated."