Looser Intel-Sharing Restraints May Be Worth a Look to Facilitate Joint Ops, Navy Data Chief Says



U.S. Sailors conduct pre-flight checks on an E-2C Hawkeye, assigned to the "Liberty Bells" of Airborne Command and Control Squadron (VAW) 115, as it starts up on the flight deck of the aircraft carrier USS Theodore Roosevelt (CVN 71) Jan. 30, 2021. U.S. Navy / Mass Communication Specialist 2nd Class Zachary Wheeler

ARLINGTON, Va. — Getting actionable, timely data to deployed expeditionary forces is tougher than keeping that data secure from prying adversaries, according to the U.S. Navy's top data official.

"We're pretty good at securing information and keeping it from people, which is the exact opposite of making it available for

decision making," concedes Thomas Sasala, chief data officer, Department of the Navy.

Enhancing data sharing is a key element in the Navy's Project Overmatch, as part of the Defense Department's Joint All-Domain Command and Control (JADC2) concept to connect sensors from all of the military services into a single network.

For years the Army, Navy, Marine Corps and Air Force have been developing tactical communications networks that can't interface with other services' networks, hampering joint operations, a pillar of the National Defense Strategy. And that's keeping crucial data from getting to front-line commanders in an actionable timeframe. It may be worth taking a look at whether security culture is getting in the way, Sasala told the Feb. 17 webinar of the C4ISRNET website's "Removing Stovepipes" series.

"You have to understand the concept of perishability," Sasala said. The information given warfighters "is generally highly perishable. And so, if that information is hacked or compromised for one reason or another, it is not useful outside its lifecycle."

Big strategic decisions are not being sent downrange for kicking-down-the door activity, Sasala said.

"Literally, it's 'This guy is on the roof right now.' And five minutes from now that information is not useful to anyone because he's no longer on the roof. And so, we have to take that risk calculus into the equation – which we don't do today."

All data is treated with the same sensitivity level, the same protection level, Sasala said, adding, it might be time to take a step back.

"The information might be classified. It might come from a highly classified intelligence source, but if it's only good

for five minutes, and only these three people need to see it, maybe we can just lighten up a little bit on how we get it to them."

However, he added, issues like keeping sources and methods secret or maintaining plausible deniability on sensitive operations have to be considered when passing data.

"It's a balancing act," he said, "more cultural than anything. There are some bandwidth restraints. There are data operability and exchange restraints, but our general risk aversion to kind of opening up the aperture a little bit on what data we send is probably the biggest barrier more than anything."

The goal of Project Overmatch is to develop networks, infrastructure, data architecture, tools and analytics that enable Navy and Marine Corps operations that swarm the sea, delivering synchronized lethal and non-lethal effects from near-and-far in every domain.

Sasala called Overmatch the maritime contribution to the broader multi-domain battle space.

"From a data perspective, data simply doesn't care whether you're Army, Navy, Air Force. Position data is position data whether it's a plane or a boat – whatever," he said. But breaking down military department silos or stovepipes "is really the key to getting at something like JADC2."