# Achieving Spectrum Dominance by Defeating the EW Kill Chain

## They may use the same tools, but don't confuse spectrum dominance with spectrum management.

BY SHAUN WATERMAN

In the peer adversary conflicts the U.S. military must prepare for in the 2020s, dominating the electromagnetic spectrum—from D.C. to daylight—will be as important, if not more, than dominating at sea, on land or in the air.

"Freedom of action in the electromagnetic spectrum, at the time, place, and parameters of our choosing, is a required precursor to the successful conduct of operations in all domains," states the U.S. Defense Department's Electromagnetic Spectrum Superiority Strategy, rolled out last fall.

As the strategy outlines, for almost half a century, U.S. military superiority has rested on its ability to operate freely in the electromagnetic spectrum, combining GPS, real-time global communications and advanced sensor capabilities to create deadly effects from ballistic missile defense systems to joint terminal attack controllers.

But something has changed. Denied the ability to use the electromagnetic spectrum, the U.S. military of the 20th century could still fight blindly and uncoordinatedly, perhaps; fight without the technological advantages that gave them an edge, for sure. But they still could fight bravely and potentially effectively. As the vision of Joint All-Domain Command and Control, or JADC2, is implemented over the next decade and the U.S. military becomes a truly networked force, that will no longer be true. In the peer adversary conflicts the U.S. military must now prepare for, it will need the electromagnetic spectrum not just to see and to communicate but to actually operate its weapons systems.

"That means resilience is more vital than ever," says Louise Borrelli, director of technology development for TrellisWare Technologies, Inc. "Above all, the U.S. military needs spectrum capabilities that will continue to operate, no matter what the enemy throws at them," she explains. "Blocking, complicating or delaying enemy efforts to exploit and/or deny use of the spectrum will be a key capability for the networked force."

But there's little empirical data about what that might require because the uncomfortable fact is, the U.S. has never been in a real conflict where its spectrum dominance was challenged. It has spent the last two decades fighting insurgent adversaries who were dangerous in many ways, but who lacked any serious electronic warfare, or EW, capabilities and were pretty much incapable of launching attacks against U.S. spectrum operations.

"Unfortunately, that's created the danger of misunderstanding about what's really needed to win and maintain spectrum dominance against peer adversaries," says Haidong Wang, vice president of product management and strategic partnerships for TrellisWare.

TrellisWare Technologies was founded in 2000 by two professors from the University of Southern California and two engineers who spun it off from ViaSat to pursue innovative terrestrial applications of cutting-edge signal-processing technology developed for satellite communications. Today, the company retains an innovative culture that strives to push technological boundaries in tactical wireless communications.

"We offer our own products, but we also provide technology for other people's products," says Wang. "Partnerships like that produce the best outcomes for the warfighter." That mindset has helped TrellisWare's technology find its way into every tactical radio set being fielded by the U.S. Army today.

At the heart of TrellisWare's DNA is engineering excellence," says Wang. "We solve the hardest problems, not because we are arrogant, but because, as a smaller player in the marketplace, that excellence is the best way to distinguish ourselves."

### Congested vs. contested spectrum

The new EMS Superiority Strategy has brought welcome attention to the spectrum challenges the U.S. military must face as it prepares for conflict with peer adversaries.

But spectrum is complex and difficult. Understanding how technologies work to deliver spectrum capabilities requires a highly specialized engineering skill set, which is rare even among the teams of policy or acquisition specialists working this issue for the Defense Department.

"Unfortunately, this can make it tough to distinguish marketing-speak from engineering know-how," says Wang.

Take the example of congested vs. contested spectrum. As the airwaves have become more crowded, spectrum congestion became an issue that any network operator will have to address. Spectrum congestion is a challenge for the U.S. military, as for any other large enterprise that must manage its use of an increasingly scarce and closely regulated resource. The advances in commercial 4G and 5G wireless technologies created an insatiable demand for more spectrum, increasing the pressure for military to vacate or share their spectrum. Many technologies have been developed that offer solutions for these problems, like interference avoidance capabilities, adaptive power control, dynamic spectrum access and multi-antenna beamforming capabilities.

Spectrum contestation, on the other hand, is a challenge unique to the military. No other network operator has to deploy capabilities able to withstand—or route around—the attacks of a capable adversary.

"The distinction between congestion and contestation isn't as well understood as it should be," says Wang.

It doesn't help that the Defense Department's new EMS Superiority Strategy aims to combine the traditionally separate functions of EW (dealing with contested spectrum) and Electromagnetic Spectrum Management (dealing with congested or constrained spectrum) into a new unified concept: Electromagnetic Spectrum Operations, or EMSO. The combination is necessary because both sets of challenges—increasing congestion and increasing contestation—have to be managed using the same EMS resources. But the new concept can also help blur the lines between two very different kinds of problems.

"The sad truth is, many of the solutions being touted for spectrum dominance might work well in the congested environments they were originally designed for; but they simply don't provide the resilience the U.S. military requires in the face of spectrum contestation by peer adversaries with advanced EW capabilities," says Wang.

"There are a lot of marketing buzzwords being thrown about," he adds. "Some of these terms are now used so broadly that they've lost any kind of definition at all. What does LPD (low probability of detection) even mean anymore?"

"There's an old joke about how a sufficiently well-prepared [technology] demo is indistinguishable from magic," says Wang. "DoD technical specialists need to take a deep dive into these spectrum technologies and employ evidence-based testing to assess their capabilities."

If they do, he adds, they'll find that:

> Adaptive power control might work to reduce interference from a network to its neighbors, but it's basically useless as an anti-jamming or LPD solution in the face of a high-level adversary.
>
> Multiple-input and multiple-output, or MIMO antenna, beamforming doesn't in reality limit emissions to narrow beams—energy is radiated in all directions.
>
> Dynamic spectrum access and interference avoidance techniques are easily defeated by sophisticated threats.

The stakes could not be higher. Misunderstanding the capabilities the U.S. military is buying means mistakes and weaknesses may not be apparent until they are deployed on the battlefield and service members' lives are at risk.

## The EW kill chain and the systems approach

To successfully challenge U.S. spectrum dominance, adversaries will need to follow the same four-step EW kill chain that our own spectrum warriors must follow.

**Signal detection**—find the channel;
**Signal exploitation**—intercept and analyze communications;
**Signal geolocation**—pinpoint the transmitter; and
**Signal denial**—jam or interrupt the messages.

Making U.S. networks resilient means understanding all four stages and deploying appropriate techniques, measures and countermeasures to defeat adversary efforts in each of them.

Spectrum resilience can be achieved by defeating or even delaying or complicating adversary measures at any stage of the kill-chain, but spectrum dominance requires defeating them all. Capabilities that are effective against advanced adversary EW capabilities—against contestation, not just congestion—need to start with a systems-based approach. They need to understand and counter every stage of the adversary's EW kill-chain with an integrated set of defenses.

"Link-level solutions only solve part of the problem," says Borelli, "which means they don't solve the problem at all. If you're only countering one or two of the kill-chain stages, you are not going to be effective. A network-level solution can oppose adversary capabilities at each and every stage."

## Delivering resilience for spectrum dominance

TrellisWare is working to develop those solutions through the whole Technology Readiness Level stack, from concept through prototyping to deployment.

• The TrellisWare TSM ™ Mobile Ad-hoc Networking (MANET) waveform is the key networking capability for the Army's Integrated Tactical Network, or ITN, Capability Set 21, currently being deployed to Infantry Brigade Combat Teams. Capability Set 21 will be deployed from 2021 through 2023 and establish the baseline that future network modernization will be built upon.

• TrellisWare has also developed a new, spectrally efficient narrowband waveform which is a fast frequency hopping MANET and complies with the Warrior Robust Enhanced Network (WREN) Narrowband (NB) Over the Air Specification. This waveform provides voice, PLI and data services and is being considered for future ITN Capability Set insertion. The TrellisWare WREN NB Waveform will allow support and interoperability among U.S. coalition partners.

• Under the DARPA Protected Forward Communications (PFC) program, TrellisWare is developing communications technologies to defeat sophisticated adversary EW capabilities and provide resilient communications to front line joint terminal attack controllers and other small units operating independently in close proximity to enemy forces.

• Under the DARPA Network Universal Persistence program, TrellisWare is helping guarantee network resiliency by separating the control plane from the data channel, enabling high capacity data channels to achieve resilient communications in challenging spectrum environments.

All of these cutting-edge solutions enable spectrum operations across a heterogeneous network, providing the fallbacks and fail-safes required for resilience. They all address capabilities from a systems-level point of view, integrating layered defense to achieve spectrum dominance in the face of sophisticated adversaries and their EW capabilities. They all live up to the TrellisWare slogan: "When Nothing Else Works ™."

TrellisWare® TECHNOLOGIES

TrellisWare works with an ever-growing community of integrators, end-users, and government stakeholders to develop the most capable tactical networking solutions enabled by TrellisWare technology. For more information contact info@trellisware.com or (858) 753-1600, www.trellisware.com