TRAINING FOR MODERN WAR

Soldiers are learning to hide their satellite dishes, while relearning basics like digging foxholes.

BY SAM SKOVE

Col. James Stultz, commander of the 101st Airborne's 2nd Brigade Combat Team, speaks with another soldier at the Joint Readiness Training Center at Fort Johnson, Louisiana, January 22, 2024.

SAM SKOVE

FROM THE AIR, the camouflaged headquarters of Maj. Gen. Jim Isenhower looked much like any other rocky hill in the barren desert landscape that surrounds Fort Irwin, in southern California.

The effect was almost perfect — except for the distinctive white square of a Starlink satellite antenna that would be all too visible to the commercially available drones used by Blackhorse, the Army unit playing Isenhower's adversary.

"Throw a blanket on that," Maj. Gen. Curt Taylor, commander of Fort Irwin's National Training Center, instructed a soldier.

As the Army absorbs the lessons of Ukraine, the service's top training centers are pushing more and more realistic scenarios on soldiers, while also giving them opportunities to try new ideas, often based on commercial tech such as Starlink.

The changes reflect the priorities of the new Army chief of staff, Gen. Randy George, who is pressing units to adapt to the increasingly surveilled battlefield and to embrace cheap, commercially available tech over multibillion-dollar weapons.

The Army has "a real sense of urgency" about operating under constant observation, George said in a January interview. Part of the solution is technology that can reduce the threat, he said at the Joint Readiness Training Center in Louisiana.

Many of these lessons are based on observations of Ukraine, commanders said.

"We have been really studying," said NTC's Taylor, who cited Ukraine's New Year's Eve strike on a Russian base located by tracking soldiers' cellphones.

Both Taylor and Col. Matt Hardman, who leads JRTC's operations group, said they were in regular contact with Security Assistance Group-Ukraine, the U.S.-led organization that coordinates international training and equipping of Ukrainian forces.

In recent exercises at NTC and JRTC, soldiers effectively entered the exercise from the moment they woke up in their home bases, much as they would in an actual war. For one January exercise at JRTC, soldiers flew some 400 miles by helicopter from their base, said Hardman.

For a February training exercise at NTC, soldiers assembled at a railhead some 40 miles away and then drove their military vehicles for the last leg of their journey, said Taylor. The old method would have seen soldiers bus into NTC, allowing them plenty of time to get their bearings.

"They get off the bus, they think they're going to bed down and go into admin," said Taylor.

The logistic portion also increasingly strives for realism. Before, units receiving artillery shells would get virtual shells. Now, they must transport mock rounds weighing the same as the real thing, said JRTC commander Maj. Gen. David Gardner.

CONSTANT SURVEILLANCE

As soon as they enter the training site, soldiers find themselves under constant observation by drone, satellite and electronic surveillance. Their cellphones become potential homing beacons for enemy forces.

Standing in a command center in the middle of the NTC desert, Maj. John Mahood said Blackhorse drones had tracked his convoy from the moment they entered the training site all the way to the command center.

"Almost the entire time that we were driving, there were small UAS systems hovering over our convoy," Mahood said. "They know we're here."

In the past, opposing forces might not strike a unit's command post. Now, to replicate the dangers seen in Ukraine and elsewhere, those same command posts may find themselves at the receiving end of a simulated missile or artillery strike.

"We have no problem doing" mass-casualties events at command posts now, said Gardner. Strikes can come as little as three days into the exercise, said 1st Lt. Seth M. Deltenre, Gardner's aide-de-camp.

NTC and JRTC have become hotbeds of technical experimentation with better ways to hide, evade, or strike back.

Soldiers with the 1st Battalion, 502nd Infantry Regiment work in their fighting positions at the Joint Readiness Training Center.

SAM SKOVE

At the most basic level, at least some command posts now come equipped with camouflage nets that also serve to dampen the electronic magnetic signature of the equipment inside.

Some units, like Isenhower's command post, are also using high-powered communications tech borrowed from the commercial world. Starlink devices can provide high-bandwidth communications in small, easy-to-use packages. Other units use Kymeta, a Starlink competitor.

Other communications tools include equipment that lets soldiers access cell networks, allowing them to hide in the mass of civilian signals and gain fast internet access.

RELEARNING OLD SKILLS

Yet some units are relearning lessons hardly changed since World War I: Low-ranking commanders must make decisions on their own; U.S. forces will be under threat from the air; soldiers must learn to dig foxholes.

For one, the risk of communications being jammed or tracked means that commanders must now become skilled at issuing clear yet simple instructions, said Gardner.

That's no easy task, said Mahood, noting that officers must now write clear, succinct orders even in stressful situations. It's also a "mental shift" for senior officers, who are used to their staff producing more detailed plans. Officers must adjust to seeing that orders are "good enough," he said.

Soldiers also have to learn to hide. At NTC, they moved their vehicles under warehouses to keep them away from prying drones and satellites, just as in Ukraine soldiers often use bridges and other buildings to conceal themselves.

Individual soldiers, meanwhile, are learning to take cover from drones in the woods of JRTC, Hardwood said.

"Rotational training units are getting better and better at camouflage cover concealment and dispersion — most importantly, in terms of the small UAS threat," said chief warrant officer Christian Lehr, a member of Geronimo, the unit that plays the Army adversary at JRTC.

Units are also doing their best to reduce the amount of equipment needed to set up command posts and are practicing taking them down quickly to prevent being easily targeted.

Capt. Charles O'Hagan of the 101st Airborne's second brigade said his unit had done an audit of the headquarters and stripped away every possible unnecessary cable. After running multiple drills, the unit shrank the time needed to break down the camp from an hour and a half to 35 minutes. The unit eventually hopes to get down to 20 minutes, he said.

And even as drones take over the sky, the infantry will still have to learn a basic skill: how to dig fast, critical for coping with artillery and other long-range fires.

"We've got to get serious about dig-or-die," said Taylor. When simulated artillery lands, "we're going to be very unkind to you as to how we assess casualties."

George's last stop at JRTC took him to the newly dug position of the 1st Battalion, 502nd Infantry Regiment company. Its soldiers had spent 10 p.m. to 2 a.m. the previous night digging foxholes in cold, wet weather in the Louisiana forest. Their camouflaged-smeared faces looked out over machine guns and anti-tank weapons. As much as drones and satellites may have changed war, they were no less tired after spending the night in a muddy hole.

"I hope they come," one soldier said as George departed. "I didn't dig this for no reason." //

"ROTATIONAL TRAINING UNITS ARE GETTING BETTER AND BETTER AT CAMOUFLAGE COVER CONCEALMENT AND DISPERSION — MOST IMPORTANTLY, IN TERMS OF THE SMALL UAS THREAT."

CHIEF WARRANT OFFICER CHRISTIAN LEHR, ARMY JOINT READINESS TRAINING CENTER

SECURING U.S. ARMY DATA AT THE EDGE

THE U.S. ARMY is looking to shift from monolithic legacy applications to highly distributed cloud and hybrid cloud environments. The challenge, however, is that it needs to do so securely, which can prove difficult.

"As the edge becomes more distributed — smaller physical locations, on the move — the protection schemes and solutions must evolve to become more distributed, which can create a larger attack surface, said Brendan Kelley, data protection & cybersecurity specialist at Dell Technologies. "The challenge is in having government-approved capabilities that can run in a hardware-agnostic environment and can also be secured while connected to the tactical edge."

To make those connections secure, the Army needs to be looking at a new generation of solutions. "They need software that does data encryption at the local source," on that distributed edge, Kelley said. "And the encryption must meet certain government security standards."

A new iteration of the Computer Hardware Systems (CHS) contract can help the Army to meet those goals. The CHS-6 contract will provide the Army and other agencies the ability to rapidly procure emerging Commercial off the Shelf (COTS) hardware and services.

"For 25 years, the Army has used CHS as a way to rapidly and securely field solutions," said Chris Gordon, area vice president of DOD and intelligence sales at Government Acquisitions Inc., which is facilitating CHS-6 procurements of Dell Technologies products.

PEOPLEIMAGES/GETTY IMAGES

"CHS has proven to be a faster way of doing procurement," he said. "With this new iteration of the contract, Army can get access to a catalog of pre-vetted products, without having to jump through hoops."

Using CHS-6, Army can leverage a number of Dell Technologies' capabilities to transition quickly and securely to a Secure But Unclassified (SBU) network.

PARADIGM SHIFT

In the past, solutions have focused on hardware, but that paradigm is shifting, Kelley said.

"You often cannot add physical [pieces of equipment] at the edge because you are limited to a certain size, weight and power capability," he said. "Dell is introducing multiple software capabilities that fit within existing hardware and that encrypt data at rest and in flight."

Within its Data Protection Portfolio, Dell has introduced two related capabilities: Data Domain Virtual Edition and PowerProtect Data Manager. "Those are two hardware-agnostic pieces of software that enable the warfighter at the edge to get the security encryption they need," Kelley said.

As the Army pivots to distributed systems such as hybrid cloud, it risks adding unnecessary complexity to its IT operations. With software-based solutions, "the goal is to streamline and automate encryption at the edge as much as possible," Kelley noted.

A modernized approach will enable those on the front lines to devote more attention and energy to higher-impact efforts. "It means that their time at the edge can be spent on actually completing the mission," Kelley said.

"Whether that mission is supporting a medical evacuation flight or a tactical operation, the Army needs to free people from the administration of backend systems," he said. "We do not want to spend more time than necessary on systems administration. When you're at the edge, you want to be able to focus on fulfilling that mission." //

PRODUCED BY Defense One

SPONSORED BY carahsoft. DELL Technologies Government Acquisitions