Army turns to smart technology to defend against threats to installations

By Joe Lacdan

Assistant Secretary of the Army for Installations, Energy and Environment Alex Beehler doesn't need proof of threats to military and government installations. He is reminded every day.

His office sits next to the point of impact where American Airlines Flight 77 crashed into the western side of the Pentagon nearly 18 years ago during the 9/11 attacks.

"It's a constant daily reminder that the Pentagon, (which) is the Department of Defense's foremost installation, clearly can be ... under a surprise attack," said Beehler.

As the variety and complexity of threats continue to increase, security at U.S. military installations has taken increased importance in the years since 9/11. Potential U.S. adversaries can threaten American bases in cyberspace and at their perimeters.

Vulnerabilites

While defending against attacks to U.S. installations has always been a priority for the Defense Department, information technology and the possibility of lethal attacks before major conflicts has made military posts more vulnerable than ever before.

"The homeland is no longer a sanctuary," said Richard Kidd, deputy assistant secretary of the Army for strategic integration. "We've been treating our military installations as if they were sanctuary cities for a very long time, immune from the effects of the adversary. That is no longer the appropriate assumption."

The Army plans to use smart technology to help defend against the increasing complexity of these security threats. Beehler said the Army needs to build a "technology-enabled" force by 2028. Lt. Gen. Gwen Bingham, assistant chief of

staff for installation management, said that has been in discussions for the past 18 months to bring 5G wireless connectivity to all of its installations.

Army installations serve an important function as the strategic support area, which is part of the service's multi-domain concept. The strategic support area features frequent communication between commanders and support agencies as well as housing crucial warfighting components such as cyber, command and control.

"Installations are really part of the battle front," Beehler said. "One of the things that you need to be concerned about: what happens when the grid goes down and there's no power on military bases or in the surrounding communities, which service the military bases?"

Smart technologies

The Army is currently exploring 10 technologies to innovate installations, including automated assessments of systems with limited manpower and monitoring utilities for anomalies in energy consumption. The service is also looking to track fault detection, install smart thermostats, and create autonomous vehicles. The Army will explore frictionless entry, allowing secure and efficient installation access.

The Army Corps of Engineers is looking at using its Virtual Test Bed Installation, which involves artificial intelligence that will analyze data of a military installation's facilities.

"The battle space is changing," Beehler said. "Installations are part of the fight. They're critical to the Army's success. They are where the Army builds readiness, sustains the force, develops Army culture (and) supports our Soldiers and families ... They are under constant attack."

Members of the 4th Infantry Division run from one building to another at Selby Combined Arms Collective Training Facility on Fort Benning, Ga., during the 36th Best Ranger Competition in April. Army installations have become more vulnerable, said Lt. Gen. Gwen Bingham, assistant chief of staff for installation management. In order to better protect Army posts worldwide, senior Army leaders said that the service will consider using smart technology to bolster security and enable commanders to respond to threats swiftly. (Photo Credit: Patrick Albright)

The possibility of threats to its installations further increases the importance of the Army's current modernization efforts. At-risk infrastructure can undermine a base's operational ability to act.

To help field new ideas for installation technological innovations, Bingham partnered with Army Training and Doctrine Command to gather feedback from Soldiers at Army training centers at Fort Lee, Virginia; Fort Sill, Oklahoma; Fort Benning, Georgia; Fort Leonard Wood, Missouri; and Fort Gordon, Georgia. The average age of the Soldier surveyed was 23 years old.

"We know that we must move quickly to adapt and change to be proactive vs. reactive and to really get ahead of technology," Bingham sad. "In other words, we want to be the driver of change vs. the passenger."

Survey Findings
Soldiers wanted the capability to access installation services 24 hours a day using biometric-enabled kiosks or mobile apps. They also wanted applications both for base information alerts and for healthy food options. Soldiers said the Army should consider using "walk out" technology where shoppers can purchase items by having a remote system scan their credit and debit cards and automatically deduct from bank accounts.

The Army could explore building the capability to counter enemy attacks against utility and infrastructure control systems. Bingham said the service could develop the means to counter against kinetic surveillance and then attack the enemy using drones and using remotely-operated sensors.

Chris Thomas, director of information and technology, Office of the Assistant Chief of Staff for Installation Management, outlined objectives to help build Army bases into smart installations capable of defending against enemy attacks.

Thomas said that industry partners must determine how the service provides connectivity and bandwidth and speed to Soldiers; new technology must be implemented sooner. Thomas said that identifying and securing operational technology will provide the ability to withstand attacks. And finally, the new technology will help provide resilience.

"We must be able to recover when these attacks happen," Thomas said. "Keep in mind it's not if we're going to get attacked. It's when. It's going to happen." ∎