

ABERDEEN PROVING GROUND, Md. -- Cyber Blitz. Cyber Quest. Cyber Innovation Challenge.

Feeling the whiplash? Good -- then hackers and attackers will, too.

Seeking to attract cutting-edge technologies from the public and private sectors as it equips a growing cyber force, the Army has established a series of events to quickly evaluate, integrate -- and in some cases, purchase -- cyber capabilities. As part of the Army's broader cyber equipping strategy, the distinct but linked events are fueling the early experimentation that leads to more agile and informed procurement.

"We have to understand what is already out there," said Portia Crowe, director of cyber operations at the Army Program Executive Office for Command, Control and Communications-Tactical. "There's a lot of capability that industry has, and it may not be specific to the Army, but we can tweak it and adapt it to what we really need it to be. So every cyber experiment we do puts us leaps and bounds ahead of where we would be if we had to develop these capabilities on our own."

Set in field and laboratory environments, the three experiments share the goals of assessing prototypes, validating concepts and informing future requirements for capabilities that will allow commanders and Soldiers to understand, detect and counter cyber threats.

Where they differ is in the operational context, specific focus areas and maturity levels of the technologies under evaluation, as well as the immediate outcomes for industry and government participants. Together, they form a broad net that allows the Army to put cyber capabilities under the microscope and in the hands of Soldiers to influence integrated acquisition and technology approaches. "Cyber Warfare is a revolution in military affairs," said Col. Joseph Dupont, trail boss for the Army Cyber Acquisition Task Force. "With that, many are working hard to enable the Army to conduct operations in cyberspace. Cyber Blitz, Cyber Quest and Cyber Innovation Challenge are not competing events. They complement each other through a partnership to inform decisions and give program managers a venue to quickly assess the operational readiness of new capabilities."

The events are as follows:

- Cyber Blitz, which held its inaugural event in April at Fort Dix, New Jersey, is executed by the Army science and technology community, specifically the Communications-Electronics Research, Development and Engineering Center (CERDEC) Space and Terrestrial Communications Directorate. Combining CERDEC's integrated modeling and simulation environment with its lab and field-based risk reduction processes, Cyber Blitz looked to address how the Army is adapting the physical construct of the main command post and interactions between different staff functions to execute cyber and electromagnetic activities. Future Cyber Blitz events, taking place twice a year, will expand to include pre-Technology Readiness Level (TRL) 6 materiel solutions focused on broad capability gaps affecting cyber and electromagnetic operations at the tactical level.
- Cyber Quest, which will conduct its first annual event in July at Fort Gordon, Georgia, is executed by the Army's training and doctrine community, specifically the Cyber Center of Excellence (CoE). Cyber Quest aims to provide a rigorous, integrated operational setting -- with a near-peer threat that reaches from the brigade to the squad level -- in order to evaluate technology solutions that have achieved TRL 6/7 status. Driven by the Army's priority cyber requirements, Cyber Quest 2016 will focus on integrating situational understanding tools for cyber and electronic warfare, as well as demonstrating tactical radios as electronic warfare solutions at the tactical edge. Next year's Cyber Quest 2017 will address other capability areas including forensics and malware detection, insider threat detection, defensive cyber operations mission planning and various tactical electronic warfare sensors.
- The Cyber Innovation Challenge, which launched in 2015 and will kick off its fourth iteration in July, is executed by the Army's acquisition community, specifically the Cyber Focal office of the Assistant Secretary of the Army for Acquisition, Logistics and Technology, in partnership with the Army Cyber

Command and the Cyber CoE. Through a vendor consortium and a flexible acquisition method known as Other Transaction Authority, the Cyber Innovation Challenge taps into small and non-traditional defense contractors to rapidly evaluate, procure and deliver limited quantity prototypes to cyber Soldiers. The Army has already conducted three formal Innovation Challenge events focused on Deployable Defensive Cyberspace Operations Infrastructure (DDI), cyberspace analytics and micro-cloud management solutions. The first DDI prototype kits, purchased from two vendors, were delivered in April to the Cyber Protection Brigade at Fort Gordon, Ga. The Army's goal is to hold three to four Innovation Challenges per year.

While the Cyber Innovation Challenge is the only one of the three events where the Army can quickly issue a contract based on the results, there are benefits to industry partners who participate in any of the experiments, said Maj. Steve Roberts, who is managing Cyber Quest 2016. Given the complexity of the military cyber environment and the culture shift taking place, vendors who participate in Army-led prototyping events will receive early feedback and collaboration opportunities that stovepiped technology demonstrations miss, he said.

"Some of the most innovative solutions are coming from vendors who have not dealt with the Department of Defense in the past," Roberts said. "So they're militarizing their capabilities, and becoming better able to provide future capabilities based on this integration effort."

Results and insights from each event are shared across the Army cyber community, influencing technology and requirements decisions as well as future experiments. Additionally, Soldiers and engineers who have participated in the events said the on-the-ground experience is already helping them, and the Army, move forward with the concepts and capabilities needed to be successful in the cyber domain.

"I'm an infantryman; I've been doing it for 18 years, but I'm having to learn a little bit of a different language as well to communicate these ideas across the cyber realm," said Lt. Col. Brent Clemmer, 25th Infantry Division, 1st Battalion, 21st Infantry Regiment Commander, who participated in Cyber Blitz. "I've walked away with this, maybe not with the depth of knowledge these experts have, but I can ask questions now of my S-6, I can ask questions now of my Electronic Warfare NCO, I can ask questions of the brigade staff and the division staff.

"The Soldiers here were able to point out flaws in the system, things that need to improve, and we were able to allow assessors to check out the process and go from there," Clemmer said. "It was a win-win."

--Nancy Jones-Bonbrest (PEO C3T) and Kristen Kushiya (CERDEC) contributed to this article.