While its creation will address an urgent need, the program’s name is a bit confusing: Persistent Cyber Training Environment (PCTE).

“It sounds like we are building an environment, which is not technically correct,” said US Army Col. Richard Haggerty, Project Manager for Instrumentation, Targets, Threat Simulators and Soft Training Systems (PMI-TTS), which is managing the PCTE program. “PCTE is really a platform with a series of capabilities or tools designed to facilitate training.”

The US Department of Defense in 2017 tapped the Army to lead PCTE, which is being managed by the Program Executive Office for Simulation, Training and Instrumentation (PEOSTRI).

Knowing how your cyber enemy thinks and being able to anticipate their next move are requisite skills for today’s cyber warrior. When operational, PCTE will help cyber mission forces “stand up, populate, execute, perform after-action reviews, then tear-down and sanitize numerous environments simultaneously,” said Haggerty. Stated another way: PCTE will help DoD to effectively plan, build and conduct cyber mission force training. The aim is to create a common and centralized training platform. Cyber mission training is decentralized for all services presently.

A few years back, the US government tasked the military to train and certify cyber warrior teams quickly, but trainers were forced to use service-unique methods, which limited the size and scope of the effort. PCTE will move those initial efforts forward by eliminating redundancies or duplication, explained Haggerty. The program also will provide a persistent and accessible training platform by hosting it on a hybrid cloud.

The addition of PCTE to DoD’s ongoing efforts to bolster cyber security within all branches of the military is needed. In October 2018, hackers stole the travel records and credit card information of 30,000 DoD service and civilian government employees. A report by the US Government Accountability Office, which reviewed government security audits from 2012 to 2017, found “mission critical cyber vulnerabilities in nearly all weapons systems that were under development.” The report noted that the cyber threat is getting worse, in part, because programs and weapons systems are operated through the Internet, where hackers troll.

The cyber threat to the military, and its civilian counterparts, has reached a critical phase where there isn’t a guidebook for training to meet the threat. “In my view, we are at a critical point of focusing on cyber training capability today versus solutions of tomorrow,” said Brett Barralough, executive director of ManTech, a cyber solutions data collection and analytics company. “PCTE is not necessarily about teaching people what to do in all situations. It is more about absorbing a higher level of education.”

ManTech is one of four tier-one vendors chosen to develop...
training tools for the first part of the PCTE program. The other vendors are Circadence, Metova and SimSpace. A full contract to fund PCTE will be awarded in FY 2020, according to the Army.

The Army set up five awards for PCTE prototyping, dubbed Cyber Innovations Challenges, or CICs. The intent of the CIC is to evaluate the technical feasibility of combining capabilities into a PCTE baseline training solution. To run the CICs, the Army is using the Consortium Management Firm for the Training and Readiness Accelerator (TReX), a modeling, simulation and training consortium. The National Security Technology Accelerator (NSTXL) is the organization competitively selected to manage the TReX consortium.

Upwards of 6,000 Cyber Mission Force individuals will train using the PCTE platform, which will be a culmination of technologies selected through the five CICs. When fully operational, PCTE will be open to all branches of the US military as well as national security-related US government agencies.

The PCTE program is unique among government and civil training programs. It does not fit into the typical academic or training program mold with a defined curriculum. There are curriculums in place already to train individuals on particular tasks for cyber protection.

PCTE could be described as an interactive, dynamic, virtual environment that also stores data for pre-event planning and post-event results analyses. Cyber warriors can view, block, monitor and fight against an attack. Training that does take place could involve individuals just out of basic training to very skilled warriors or teams which are training for an upcoming mission.

“Think of it as medical training,” said SimSpace CEO William Hutchison, by way of an analogy, “where you can rehearse surgical operations by providing the medical instruments, the nursing staff, the operating room and the virtual patients.” SimSpace CTO and co-founder Lee Rossey added, “The goal is to not replace the school house. But there is an assumption of competency by the operators, who know the basics of cyber.”

PCTE is meant to be more self-paced for the individual and teams. The emphasis is less on instructor-led training and more on the environment and the team level, said Rossey.

Because there was no blueprint, the Army involved users in their prototyping efforts and early development. While the requirement document was being codified, “we got in some streamlined prototyping,” said Haggerty. The incremental capability of the second prototype was to be released in January or February 2019. Which, when completed, will provide limited training capability and inform the training requirements. A third prototype will be delivered this July.

The next user assessment will come in early 2019. The main focus is getting the base architecture and training platform in place. The Army is running 30-day,
software development “scrums” as part of their development process. “This is an industry best practice, and I don’t think the government does this kind of thing very often,” said Haggerty, who credits the cooperation among the four vendors as a principal reason for PCTE’s quick development.

The PCTE program has not followed the typical procurement path for government programs, which can be tedious and confusing. Funding for PCTE was based upon a critical need and some was provided upfront. There wasn’t even a program office early on when the seed money started coming in, said Haggerty. The proposed $800 million PCTE contract runs for eight years, with nearly $500 million presently earmarked, said Haggerty. Additional funding will be provided to fund hardware and software solutions. But is it enough to meet the threat?

“PCTE is needed. But they [the US government] are not putting enough money into the effort,” said Richard Sterk, group leader and senior aerospace/defense analyst, Forecast International. “Compared to Russia, China and Eastern European countries, the US is way behind in cyber warfare.”

One problem DoD and its civilian counterparts are having is that “you can never make a computer system child-proof,” said Sterk. “The only way to fully protect your system is not to have it networked and there are pros and cons to that strategy.” He added: “The more you network, which is where the US is going, the more you open yourself up to attack.”

While the US government does not have a separate standalone agency to handle cyber threats, PCTE could help lay the groundwork for such an effort. Much of the funding for PCTE and other initiatives goes directly to the US Cyber Command, one of 10 unified commands of DoD.

Even when PCTE becomes fully operational, the overriding challenge of keeping ahead of the evolving threat remains. Cyber has been around since the 1980s, but the threat is now global and more sophisticated. As such, cyber warriors remain students throughout their careers regardless of their level of proficiency.

Asked Haggerty: “How do you train somebody in something that is changing so drastically and dramatically? That has influenced our strategy. We want to make sure that we are not lagging behind, not putting in place a training platform that will be obsolete 12 months after we deliver it.” Another consideration: the rules of cyber engagement remain undefined, amorphous. And that puts military commanders in an awkward position of whether to train defensively, offensively or both. PCTE will help create better training and performance methodologies for cyber warriors, according to its developers.

Keenan Skelly, vice president of global partnerships and “security evangelist” for Circadence equates cyber warfare to her former occupation as an explosive ordnance disposal technician. “In Iraq and Afghanistan, the enemy was changing the explosive devices regularly. From day to day, you didn’t know what kind of device you were working on. You had to be able to think on your feet and come up with a new solution.”

She added: “What we’re doing in cyber is very similar. We’re never going to have the answer for every solution. But we can provide our cyber warriors with helpful knowledge and tools that, when they’re faced with something new and unrecognizable, they are able to deal with it.”

While PCTE is a standalone program, there are other related initiatives that share the goal of reducing the cyber threat. The National Cyber Range (NCR) complex, which is sepa-
rate from PCTE, and evolved out of a Defense Advanced Research Projects Agency (DARPA) program, also is managed by Haggerty’s office. For now, the government-owned NCR program operates out of a Lockheed Martin facility in Orlando, Florida. In time, the PCTE could leverage the NCR capabilities to support training and reduce program costs and manpower. Based on the growing need for cyber training and tests, Congress provided funding for NCR through the National Defense Authorization Act. NCR is a 10-year program that could add four or five different locations eventually.

The increased use of artificial intelligence (AI) is also part of the Army’s efforts to combat the cyber threat. An adjunct to PCTE is the Automated Cyber Opposition Forces (OpFor), which derives from the Small Business Innovation Research (SBIR) program. The initiative is meant to enhance defensive capabilities training of the Cyber Mission Force (CMF).

“We are looking for an improving opponent based on artificial intelligence and machine learning that would be able to react to the defensive actions of the CMF and require greater understanding and higher-level actions by cyber warriors,” said Haggerty. “The long-term intent is to harness prototype capabilities within the PCTE platform and define the PCTE infrastructure requirements to harness automated cyber OpFor as well as automating recommended training to overcome training gaps.”

The Central Florida Cyber Center of Excellence is one of Haggerty’s ideas to grow cyber technical capability and connectivity within the local Orlando and Central Florida area. Recent efforts include hosting cyber “Hackathons,” which include the participation of local schools, businesses and government organizations, under the Team Orlando Cyber banner. Building a classified facility also is on the wish list, said Haggerty.

**The Cyber Training Vendors**

Circadence offers a number of cyber related products and services. One core product offered for PCTE is Project Ares, which Skelly describes as a “gamified, persistent cyber training environment powered by artificial intelligence.” [Ares is the God of War in Greek mythology.]

The cyber security training and assessment platform imitates actual networks using real-time threat intelligence and provides machine-learning games to educate cyber warriors. The gamified platform, available 24/7 via web browser, increases knowledge and skills retention to 75% compared from only 5% with traditional classroom training environments, Circadence claims.

ManTech is providing planned network, schedule training and deploy environment capabilities for PCTE. The company is helping the Army erect a unique physical and virtualized computing facility, providing infrastructure and integration support with its Open Microservices Enterprise Framework. Subcontractor Ultimate Knowledge Institute (UKI) is providing the EMF 360 learning management system (LMS) for cyber training. The LMS supports instructor-led or self-paced online courses for students worldwide. ManTech also delivers online courses, certification exams and social media training. Among the exercises for students is putting them under “live fire” by actual malware on safe replications of their networks and training them in tactical response.

Boston-based SimSpace is developing an order portal and content repository for the PCTE program that will enable students, members of the Cyber Mission Force (CMF), to access the PCTE platform and associated training aids. At present, CMF scenarios are deployed manually on a variety of cyber ranges. SimSpace produces a cyber range to conduct advanced cyber training and testing. The company offers solutions with fidelity, interoperability and reusability and, like its competitors, was awarded its contract through the competitive CIC.

Privately-held Metova Cyber CENTS will support PCTE through cyber range-related technologies: Blue Space, which focuses on establishing cyber key terrain; Grey Space, which supports commercial and DoD information network architectures; Traffic Generation and Threat Emulation, based on Metova’s SLAM-R technology, and Cyber Integration with Warfighter Platforms, based upon Metova’s research in cyber integration for multi-domain battle and includes the integration of modeling and simulation, electronic warfare, intelligence and kinetic domains. (Metova is a Service Disabled Veteran-Owned Small Business.)“PCTE is the best of breed solution that will be the platform on which all cyber mission forces are trained mission-qualified,” said Kevin Hofstra, chief technology officer, Metova Federal.

The need to safeguard against cyber-attacks against the US government and agencies through better training technologies and methodologies is expected to continue at a faster pace, though doctrinal and organizational challenges remain. PCTE is one program DoD is counting on to reduce cyber threats to all branches of the US military.