ManTech
Securing the Future

On-demand Cyber Training

The Key to Beating Perpetual Cyberattacks

A ManTech White Paper

The cyber domain is like any other military or intelligence theater of operations: Success requires highly skilled, well-trained and experienced professionals.

Technology in the form of advanced systems, tools and software are indispensable, and staying ahead of adversaries requires constant innovation. But just like any weapons system, ordnance or strategic plan, the best technology is of limited value without the people to make it work at its highest level. We recruit and train pilots for new generations of aircraft; we must do the same for cyber warriors.

Not enough people with proper cyber skills exist to meet the nation's current needs, which will only grow in the future along with the threat. Cyberattacks provide relatively easy and inexpensive ways for adversary governments and criminal organizations to endanger the United States via disruption of our U.S. military command-and-control systems and critical infrastructure.

Our adversaries are actively building their cyber capacities, and we must do the same. The challenge is to find, recruit and train a generation of cyber professionals, and to do so as quickly as possible. The question is how.

Training people properly requires several well-thought-out components, all of which must work together as a seamless whole:

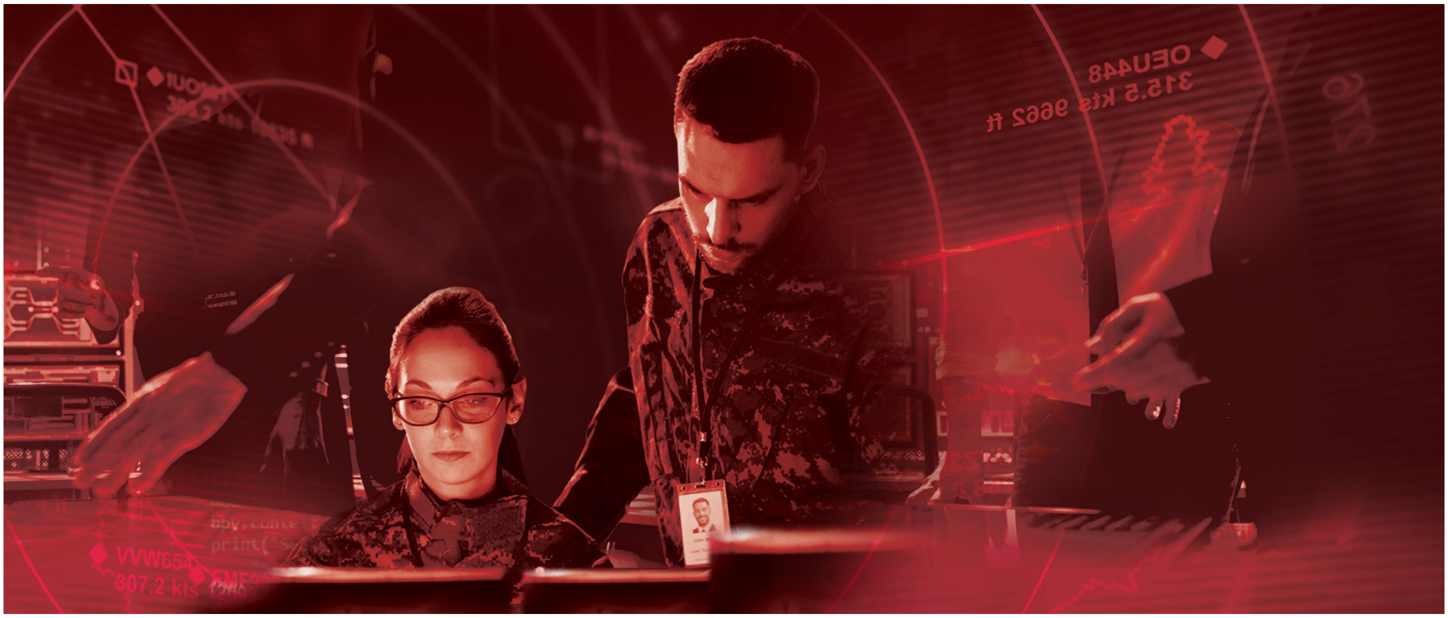
- A purpose-built cyber range and learning management system that can manage a globally-distributed user community and on-demand cyber training environment infrastructures.
- A flexible infrastructure that trains cyber warriors to secure a multi-domain battlefield and adapt quickly to changing requirements and environments.
- Strong testing to ensure that systems are cyber-hardened and personnel are equipped to fight in the cyber domain.
- The ability to train all personnel in offensive and defensive cyber, because the most effective defense is informed by a thorough understanding of offensive cyber operations.
- An insider-threat capability designed to defend the network as a complement to the external threat.
- A trusted and reliable partner to design, build and sustain government cyber ranges.

The Training Environment

The training environment should serve as a one-stop shop that can manage a globally distributed user community and range infrastructures, and allow for rapid response, escalation, and remediation services for training, exercises, and the range's authoritative record stores.

All exercise participants should have one primary interface to the exercise environment that directly supports use cases surrounding war gaming "blue team" and "red team" actions. The interface dynamically creates views into the environment tailored to the specific user's exercise roles, including allowing for white cell, or administrator, participation. Event support requires an administrative control channel so that geographically distributed white cell and help desk personnel can quickly communicate.

Systems administrators and support personnel for technical operations need a common operating picture as their primary interface to monitor system



health and status. In addition, the environment should dynamically generate views and accesses for users based on their roles, which can vary from event to event. Individual participants may be involved with multiple events or exercises simultaneously, often with different roles, and should be allowed to dynamically select among the events to which they are assigned and receive content appropriate to their roles.

Experience tells us that cybersecurity training is complete only when participants are trained in both attacking and defensive roles. A cyber range is a two-way live-fire exercise. Honing user skills in offensive cyber lets participants better anticipate and recognize adversary actions. Similarly, participants benefit from a thorough grounding in insider-threat detection. These scenarios can be integrated into any training exercise to provide a realistic environment to recognize threats from within.

Users need realistic and meaningful visualization in an exercise, regardless of their roles. In order to maintain a realistic experience for active participants, white cell observers and non-technical personnel need a customized visualization.

System Requirements

Systems vary within the DOD, and the range environment should be able to work within the evolving system of each service or command. The better option is to integrate mature, commercial off-the-shelf capabilities with existing infrastructure designed to take advantage of current capabilities while developing new ones.

Another key point: Operations & maintenance programs should be vendor-independent and open-source to ensure efficient upgrading and lower operational costs. These two vital characteristics allow for rapid customization to accommodate changes in the threat environment and to incorporate innovations that become available over time.

Systems must be scalable and severable, and able to extend from local to global operations and from individuals to large groups. To ensure maximum adaptability, all components should be “snap-on” and “snap-off” to accommodate development and execution of diverse training scenarios.

Finally, organizations should embrace automation to see detailed information on configuration throughout the cyber defense environment and accelerate access to critical intelligence. With automation in place, users spend less time on routine troubleshooting and can focus on what counts: making their cyber training proactive in detecting and stopping a wide range of sophisticated, persistent threats that emerge by the moment.

The Need for Persistent Cyber Training

As has been well-documented, a new form of malware emerges every 3.2 seconds. Add to this the multitude of cyber risk variants – DNS hijacking, spear phishing, ransomware and bots, to name but a few – and it is clear that the peril of cyberattacks accelerates not just by the day, but by the moment. The threat grows even more serious with the emergence of artificial-intelligence-driven cyberattacks that mutate when rejected by cyber defenses until they find a vulnerability that grants them access. The only proven method of defense against such a dynamic threat is offense-informed defense that evolves even faster.

The attackers are evolving, too, as hostile nation states surpass criminals and lone wolves as the most dangerous foes in the fifth domain of today's battlespace. Increasingly, foreign militaries lead the charge. According to U.S. government and news media reports, forces aligned with Russia's military are widely assigned responsibility for attacks in Ukraine, including one that brought an important bank's IT system crashing down in 48 seconds. In China, cyber-sophisticated military commands, including the notorious People's Liberation Army Unit 61486 and Unit 61398, dedicate their days to penetrating and compromising Western defenses, as well as our critical infrastructure industries, according to reports in The New York Times.

In this environment, intensive ongoing cyber training remains the most important weapon for safeguarding America's military might and the institutions and democratic way of life we stand for.

To defeat the shape-shifting hydra of persistent threats, our cyber warriors must be more determined and flexible than their foes. Cyber training has changed and requires real-life modeling and simulation environments with hands-on experience that builds on their knowledge daily.