Wrap Up: Cyber Shield 2018

By LTC BE Rhodes, Colorado Army National Guard

The hacktivist group was angry about the tolls and fees on the new "National" road. Playing on public perceptions, the hacktivists began an information campaign using social media against the company responsible for building, installing, and maintaining the toll systems. Using open source tools and techniques, the hacktivists began probing their target finding multiple vulnerabilities that could be easily exploited. Upping the ante, the hacktivists turned to a cyber-criminal element to hold the target company's data at risk, posting stolen data online. In the background, an Advanced Persistent Threat (APT) was there all along, quiet and nearly undetectable watching the whole show...

Sound farfetched? Everything described just happened during Cyber Shield 2018 in May at Camp Atterbury, Indiana. The Blue Teams included personnel from the National Guard and Army Reserve. Cyber Defenders from every team worked with a civilian Network Owner to assess the problem set, conduct network security monitoring (NSM), and tangle with a live Opposing Force (OPFOR). In total, more than 800 personnel from across the United States and its Territories participated in the most successful Cyber Shield to date.

Cyber Shield 2018 participants battle it out in NetWars at Camp Atterbury, IN

This was the seventh iteration of Cyber Shield providing a technical skills assessment to the participating Blue Teams. Cyber Shield is planned and executed by a volunteer staff from across the National Guard and Reserves. Personnel in the primary staff roles and work groups spent hundreds of hours of their own time creating a realistic scenario, generating standard Army orders products, building on range* assets (servers, applications, databases, etc.), serving at the discretion of Senior Leaders in their home organizations. Without the passion of these unsung heroes, Cyber Shield would not exist nor provide the significant training value realized each year.

Cyber Shield is the Annual Training (AT) event for multiple organizations from across the National Guard and Reserves. Many of the Cyber Shield participants spend additional weeks and months each year training on advanced skills, maintaining professional certifications, and preparing for potential missions. Soldiers and Airmen spend a week training in their assigned work-role tracks, honing their skills in preparation for getting on the "range" (in the context of Cyber Shield, range equates to Cyber Range, a self-contained information technology testing environment). At the end of training week, teams competed in SANS NetWars for the "glory" of their home states. In addition to NetWars, Cyber Shield hosted a "Cyber Fair" where many of the event participants showed off their skills in Coding, Hacking, Making, and an Open category.

On Sunday, the entire exercise gathered for the mission-in-brief. The Blue Teams were presented with the story above and told their mission had a "life safety nexus" due to Cyber threats around the Nation. Game on!

Participants receive their mission in-brief at Cyber Shield 2018

The challenge facing the Blue Teams was not an easy one. First, they had conduct a vulnerability assessment on a very exposed and broken network. In addition to figuring out what was going on in Network Owner's network and systems, Blue Teams had to actively defend their own "zone" which contained the tools they needed to attempt to discover the OPFOR's handiwork. The next step for the Blue Teams was to assist the Network Owner in setting up NSM. Just like in many environments, the Network Owner had many high-end open source NSM capabilities that were not configured. Defenders had to rely on their training all while working to build situational awareness in the blind. Finally, by the third day on range, the Network Owners had seen enough, asking their supporting Blue Teams for assistance in reducing the effects of the threat actors. Working in concert with the Network Owners, Blue Teams began conducting measured mitigations to slow down the multiple OPFOR threat actors who had invaded the network and systems.

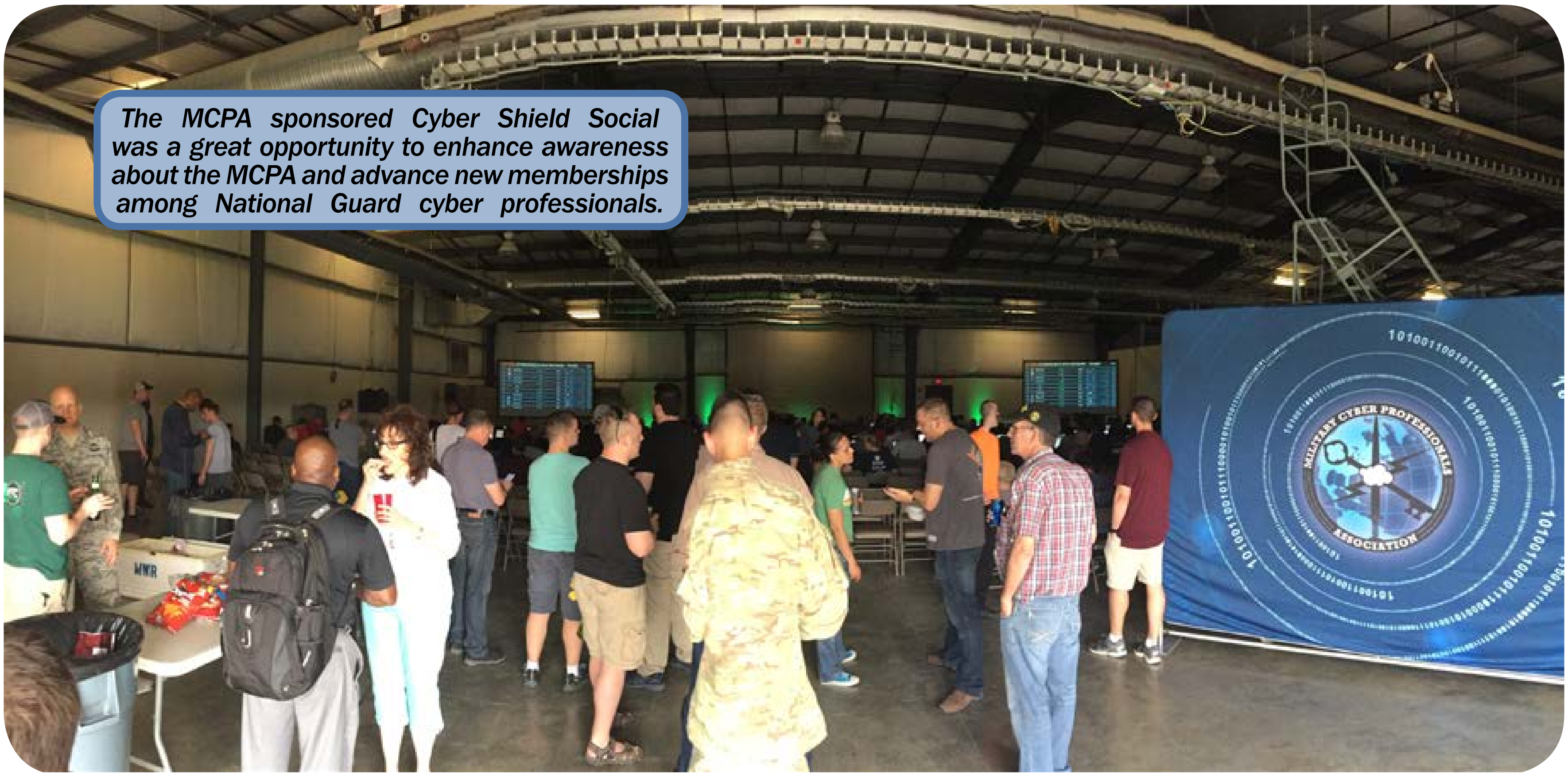
Defenders in the fight at Cyber Shield 2018

The true goal of Cyber Shield is that every participant walks away having learned something new, while improving their skills. At the end of the exercise each Blue Team walked away with an assessment of their technical capabilities. The Cyber Shield Exercise Officer-in-Charge, COL Teri Williams (Ohio Army National Guard) summed up this year's event: "**Cyber Shield is truly a crucible where industry cyber talent merges with our military forces and the result is a more polished, tuned, and stronger response capability.**" With the Cyber threat landscape expanding daily Cyber Shield continues to deliver a realistic training experience for Defenders on the front lines of their States and the Nation.

LTC BE Rhodes leads an Army National Guard Cyber Protection Team. In his civilian job, he is a Cybersecurity Professional for a global consulting firm. He has more than 20 years of experience in cybersecurity, the DoD, Intelligence Community, and industry. He is a CISSP, CEH, CCNA Cyber Ops, CNDA, Security+, and GIAC-GLEG. BE is a founding member of the MCPA-Denver Chapter. Follow him on Twitter @cyberguy514.

MCPA Was Proud to Host the Cyber Shield Social!

Military Cyber Professionals Association (MCPA) hosted a social during Cyber Shield 2018. This national-level exercise involved more than 800 participants in one of the largest US National Guard's cyber-operations exercise. Participants include members of the Army National Guard, Air National Guard, Army Reserve and representatives of State and Federal government agencies, Industry partners and Academia taking part - to test their collective skills and evaluate their defensive capabilities in response to cyber warfare. The MCPA sponsored Cyber Shield Social was a great opportunity to enhance awareness about the MCPA and advance new memberships among National Guard cyber professionals. The event helped kick off the subsequent SANS NetWars tournament, where 32 teams battled for the top position. Teams consisted of five cyber warriors from various backgrounds including: military, government, and private sectors.


The MCPA sponsored Cyber Shield Social was a great opportunity to enhance awareness about the MCPA and advance new memberships among National Guard cyber professionals.

For more on Cyber Shield 2018:

DoD: National Guard Conducts Annual Nationwide Cybersecurity Exercise
https://www.defense.gov/News/Article/Article/1520257/national-guard-conducts-annual-nationwide-cybersecurity-exercise/

Senior Leaders Meet to Discuss National Guard's Role in Cyber Warfare at Cyber Shield 18
https://www.dvidshub.net/video/601377/senior-leaders-meet-discuss-national-guards-rolecyber-warfare-cyber-shield-18

National Mock Cyber Attacks as Part of Cyber Shield 18
https://www.army.mil/article/205672/mock_cyber_attacks_as_part_of_cyber_shield_18

Interview of MCPA Member, LTC Brad Rhodes, Cyber Shield 18 Deputy Officer-in-Charge
https://www.dvidshub.net/video/601829/cyber-shield-18-exercise-week-broll

Additional Articles, Images, and Videos on Cyber Shield 18
https://www.dvidshub.net/feature/CyberShield18

All image credits: Cyber Shield PAO