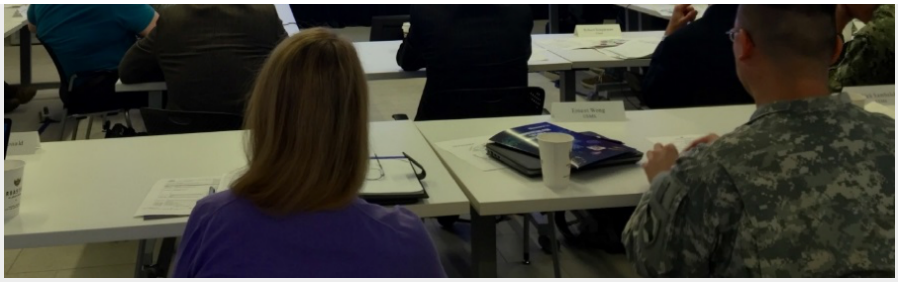
Indiana Exercising Plans to Combat Cyber Threats: Preparing for CRIT-EX 2016

By CPT Mike McDonald, Doug Rapp, LTC Ernie Wong | May 06, 2016

On the 21st and 22nd of March, 2016, Indiana hosted its inaugural Defense Cyber Summit (DCS), which aimed to advance the state's cyber readiness and preparations against a cyberwarfare attack. Spurred on by Admiral Michael Rogers, the Commander of the U.S. Cyber Command, who in 2014 called cybersecurity "the ultimate team sport," Indiana has purposefully adopted a culture of collaboration between government organizations, private firms, non-profits, and academia to improve the state's response and resiliency to a significant cyber incident. This team approach will counter cyberattacks intent on degrading Indiana's economic capacity and threating the critical services of its citizens [1]. Under the umbrella of the Applied Research Institute (ARI), organizations such as Purdue University, Indiana University, Crane Naval Surface Warfare Center, the Cyber Leadership Alliance, the Indiana National Guard, and the Indiana Department of Homeland Security have partnered together to address and propose solutions to Indiana's cyber security challenges. This effort is boosted by the Indianapolis-based Lilly Endowment support of nearly $16.3 million that is funded through a grant from the Central Indiana Corporate Partnership Foundation. The ARI is working to foster collaboration, research, and problem solving on cyber threats to Indiana's critical infrastructure [2].

Purdue University Professor Joe Pekny welcomes attendees to the Inaugural Defense Cyber Summit (photo by Tony Chase)

The DCS concept was conceived during visits to US service academies by an Indiana delegation. Representatives from Purdue's Burton D. Morgan Center for Entrepreneurship, the Purdue Research Foundation, and the Cyber Leadership Alliance, had originally concentrated on partnering Purdue University with the service academies in order to provide the most cutting-edge knowledge and technology to future cyber warfighters. "It didn't end up that way," professed Chad Pittman, Purdue Research Foundation's Vice President for the Office of Technology Commercialization. "We realized there was a bigger need here so we brought together even more problem solvers looking into improving our cyber resilience and expanded the audience to include all cyber forces in defense," Pittman continued. Upon reflecting on just how many more participants and organizations the delegation would be partnering with, Pittman jokingly remarked, "Despite having a lot of corn in Indiana, we don't all work in silos."



DCS attendees listen to Indiana University Professor Steve Myers (Photo by Michael McDonald)

While total prevention against a cyberattack is not possible, the DCS has bolstered the understanding that healthy cyber hygiene practices, and relatively inexpensive cyber protection measures can provide enough prevention that the incidence of successful attacks becomes manageable. Furthermore, the summit emphasized that it takes not only technical means to help monitor and detect a cyber threat, but, perhaps more importantly, a network of people with sound processes to quickly, effectively, and efficiently respond to the determined actions of an active and intelligent cyber adversary. Finally, a robust intelligence sharing architecture helps to immediately alert key nodes in our cyber ecosystem of an attack so it can be treated at a localized level as possible rather than become overwhelmed by a sufficiently broad attack; consequently, the initial stages of recovery can begin to restore people's trust and confidence in the security of our cyber infrastructure. All these discussions at the DCS are consistent with the prevailing US Department of Homeland Security construct on cybersecurity (see Figure 1).

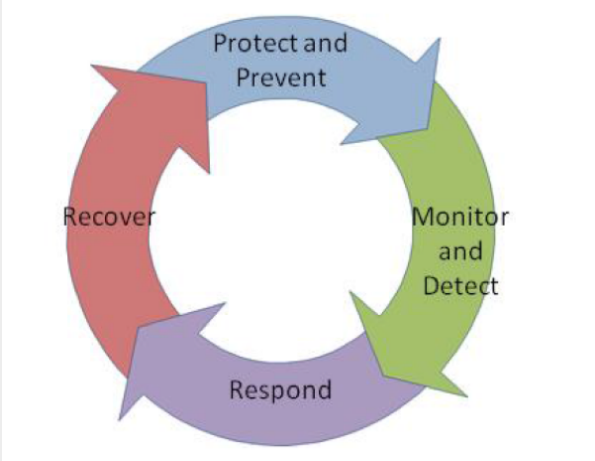


Figure 1: US Department of Homeland Security's Prevailing Cybersecurity Construct [3]

Purdue Computer Science Professor Mikhail Atallah summarized Indiana's approach to cybersecurity best when he articulated his research team's philosophy on improving anti-counterfeiting of digital media through innovative cryptographic methods: "What we are simply trying to do is to make it harder for adversaries to attack our systems; and this is particularly effective when it costs us just a little bit more to succeed while disproportionately increasing the expense for the adversaries in their attempt to win." By applying Professor Atallah's sensible proposition to the notional taxonomy of cyber adversaries that the US Defense Science Board has introduced (see Figure 2), we can reduce the likelihood of cyberattacks from every threat tier. If we can systematically increase the cost for cyberattacks to succeed, we can diminish nuisance threats operating at the lower levels using malicious code developed by others or exploiting pre-existing known vulnerabilities, but also make it more difficult for those existential cyber threats at higher levels that create new vulnerabilities in our otherwise adequately protected systems through full spectrum techniques, such as acquiring unauthorized access through blackmail and bribery, or employing proximate physical or electronic means for gaining system penetration. The innovative thinking and research into complex cyber challenges taking place at its universities are a strong testament to Indiana's marketing campaign of "A State that Works."

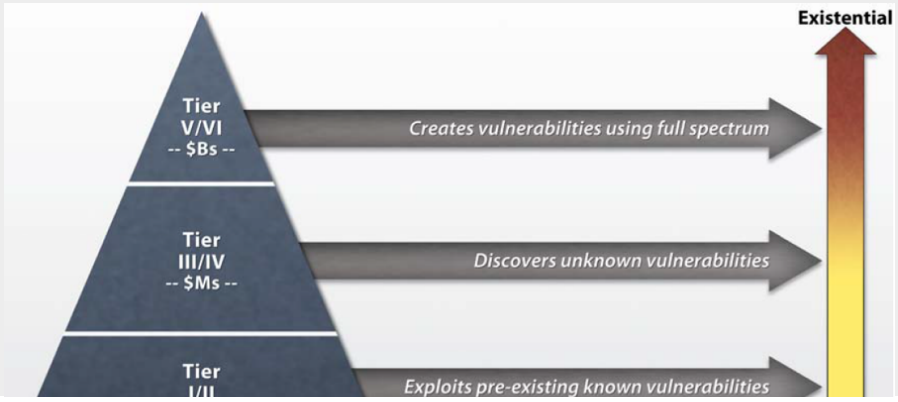


Figure 2: US Defense Science Board's Notional Cyber Threat Taxonomy [4]

The DCS was attended mostly by experts in cyber-related fields, to include academic scholars informing the attendees of their research into cutting-edge solutions to cyber challenges, and cybersecurity authorities explaining their collaborative procedures, methods, and tools to help protect against, and respond to a critical cyber incident in Indiana. One of the most noteworthy commentaries at the summit, however, was delivered by Carolene Mays-Medley, the Commissioner and Vice Chairman of the Indiana Utility Regulatory Commission. Her appeal for Indiana to be better informed of cyber threats that can significantly impact not just our individual privacies, but also seriously cripple basic services that we collectively depend upon on a daily basis, such as electricity, water, and telecommunications, resonated splendidly with the audience. But unlike most cybersecurity conferences where cyber-experts preach mostly to one another—a group of like-minded individuals already cognizant of the need to be vigilant with increasing dependence on digitally connected technologies—Comissioner Mays-Medley readily admitted that she is a technological neophyte who only recently gained an appreciation for the enormous dangers and significant vulnerabilities our digitized society has with the continuously expanding internet. With key government officials championing this cause and promoting the need for better cybersecurity, Indiana is ensuring that it has created cooperative partnerships that can plan and prepare for a broad-scale cyberattack, and can successfully practice, rehearse, and continually improve how it employs cyber best practices for the collective good of the entire state. Through the DCS, Indiana is showing that it is on the right path to making sure the state is cyber-resilient.

DCS Participants board a UH-60 Blackhawk en route to the Muscatatuck Urban Training Center (Photo by Doug Rapp)

Indiana will be hosting Crit-Ex 16.2 on the 18th and 19th of May, which allows participating organizations from across the public and private sectors to improve their understanding of the cyber ecosystem [5]. Crit-Ex officially launched in March 2016 with a tabletop exercise (TTX) held at Camp Atterbury, during which exercise players discussed their response to a coordinated cyberattack on Indiana power generation and transmission facilities. With the lessons learned from the Crit-Ex 16.1 TTX, the Indiana Department of Homeland Security in conjunction with the Indiana National Guard, Indiana Office of Technology, Cyber Leadership Alliance, and over 16 other public and private partners have developed a controlled functional cyberattack exercise that will allow participants to deploy resources and communicate with response partners to mitigate adverse effects and expedite recovery. With expert teams executing a real-world attack on a "production" water utility SCADA system located at the Muscatatuck Urban Training Facility, exercise participants will gain an enhanced understanding of their protective, response, and recovery postures, and provide additional insights into gaps in communication, resources, and coordination. The purpose of Crit-Ex 16.2 is to improve the overall security and responsiveness of Indiana's critical infrastructure in the event that an advanced cyberattack disrupts basic essential services and presents a public safety threat. Through its Defense Cyber Summit and upcoming Crit-Ex, Indiana is showing why it considers itself to be the Midwest cyber center of gravity.

Notes

[1] C. Roulo, "Cyber Defense a Cooperative Effort, Rogers Says," DoD News, Defense Media Activity, November 15, 2014. Available at http://www.defense.gov/News-Article-View/Article/603656.

[2] D. McGowan, "Lilly Endowment Pumping $42M Into Southwest Central Indiana," Inside Indiana Business, December 23, 2015. Available at http://www.insideindianabusiness.com/story/30812018/lilly-endowment-pumping-42m-into-southwest-central-indiana.

[3] US Department of Homeland Security, "Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action," March 23, 2011. Available at https://www.dhs.gov/enabling-distributed-security-cyberspace.

[4] US Defense Science Board, "Task Force Report: Cyber Security and Reliability in a Digital Cloud," January 2013. Available at

[4] US Defense Science Board, "Task Force Report: Cyber Security and Reliability in a Digital Cloud," January 2013. Available at http://www.acq.osd.mil/dsb/reports/CyberCloud.pdf.

[5] Indiana Department of Homeland Security and Cyber Leadership Alliance, "Crit-Ex 2016: Advancing Cybersecurity for the State of Indiana," fact sheets 1 and 2, January and April 2016.