Peraton | **LABS**

Peraton Labs Overview

Alexander Poylisher

Scientific Research/Analysis Senior Manager

apoylisher@peratonlabs.com

Ritu Chadha

Senior Research Director

rchadha@peratonlabs.com

About Peraton

- **Impacting missions of consequence across the globe…**
  - National intelligence collection, analysis & dissemination
  - Full spectrum cyber operations and information dominance
  - Space protection & resiliency
  - Secure, resilient global communications
  - Border and maritime security platforms
  - International coalition strike platforms
  - Hypersonic weapons
  - Foreign Affairs
  - Citizen health and safety
  - Mission-based enterprise IT modernization
- **…and deep into the far reaches of the galaxy**
  - Human space exploration

~18,000	~50%	20%	70
Employees	Cleared employees ~16% TS/SCI	Military Veterans	SCIFs (53 accredited, 17 under construction)

Peraton | LABS

Peraton Labs Overview

Peraton Labs delivers the future across cybersecurity, communications, mobility, electronic warfare, and analytics to government and commercial customers worldwide

- Organization created in 1984 after the breakup of AT&T and Bell Labs, expanded with the addition of DHPC Technologies, and acquired by Peraton in 2021
- Long tradition of developing innovative technologies
- Extensive research collaborations with elite universities and leading-edge companies and startups
- Leadership positions in 20+ standards bodies and professional organizations

470
scientists, engineers and analysts on staff

25%
of our technical staff are patent inventors
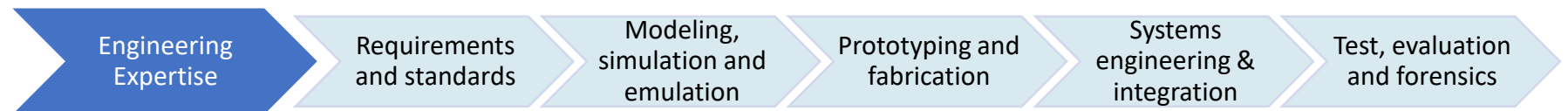
50%
of technical staff with master's; 30% PhDs

75%
of our technical staff hold gov't clearances

Peraton | LABS

In 2021 Perspecta is acquired by Peraton, a next generation national security company with ~20,000 employees serving high-consequence missions on a global scale

Bell Laboratories
Originally part of AT&T Bell Labs

APPLIED COMMUNICATION SCIENCES
Spun-off as ACS and bought by The SI in 2013

perspecta LABS
Perspecta launched as a public company in 2018.

1980	1990	2000	2010	2015	2020	2021

Telcordia
Became Bellcore/Telcordia during 1984 Bell System divesture

VENCORE LABS
Rebranded as Vencore Labs after The SI's purchase of QinetiQ North America in 2014

DHPC TECHNOLOGIES
Acquired DHPC Technologies, a leading provider of innovative electronic warfare solutions.

Peraton | LABS

Technical Capabilities Summary

- Majority of staff located in multiple sites in NJ, MD and VA, including:
  - -- Basking Ridge, NJ
  - -- Picatinny, NJ
  - -- Aberdeen, MD
  - -- Silver Spring, MD
  - -- Fort Belvoir, VA
- Facility in St. Louis for Display Technologies

- Markets served:
  - -- Defense & intel
  - -- Civilian agencies
  - -- Utilities
  - -- Transportation
  - -- Life sciences

Cyber-security	Electronic warfare	Machine learning and AI	Mobility & wireless systems	Sensors & sensor integration	Optics, photonics & quantum	Networks and operations
Cyber defense and cloud security	EO/IR/RF technology	Machine learning techniques	High performance RF comms	Sensor / laser instrumentation	Optics and optical networking	Network control and service mgmt
Cyber warfare	Attack, protect and counter-measures	Adversarial Machine Learning	Signal processing applications	Spectrum sensing and management	Photonics system design and integration	Network architecture and protocols design
Critical infrastructure protection	Threat detection	Data correlation, fusion and integration	Wireless network management and security	Systems architecture and sensor integration	Applications of advanced laser-based technologies	Software defined networks
Vulnerability and risk assessment	Counter-IED/UAS	Cyber and wireless analytics	Secure mobile comms	Controls and automation	Quantum comms and computing	Network virtualization

Engineering Expertise → Requirements and standards → Modeling, simulation and emulation → Prototyping and fabrication → Systems engineering & integration → Test, evaluation and forensics
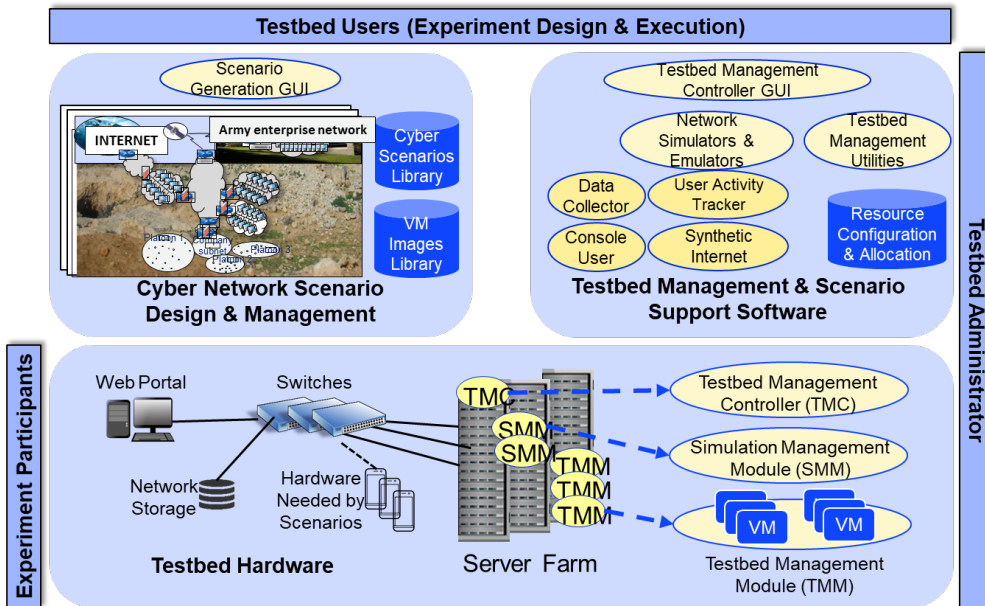
Peraton | LABS

Peraton Labs has a long tradition of R&D leadership for Government agencies

- Top performer at DARPA
  - Large number of ongoing programs in I2O and STO, e.g.:
    - LINC, CHASE, OPS-5G, GARD, REPO, D3M, RACE, ConSec, FastNICs, SDCPS (I2O)
    - CONCERTO, DyNAMO, LogX, Network UP, SHARE, MINC (STO)
    - Multiple classified efforts (I2O and STO)
  - Other: SAFE-SiM (ACO), CODE, TMVD (TTO)

- Prime performer on IARPA Trojan AI, COVID-19 seedling program

- Multiple large ongoing programs with Army agencies, e.g., DEVCOM C5ISR Center, DEVCOM Army Research Lab

CyberVAN: Flexible, Scalable Cyber Range

- **Funded by DEVCOM Army Research Lab**

- **Program Goals:**
  - Develop, maintain, and enhance **CyberVAN**, Peraton Labs' innovative tactical experimentation environment that:
    - Provides **high-fidelity representation** of enterprise, strategic and tactical networks including a comprehensive library of network models, cyber effects, traffic
    - Allows running tactical applications in native environments with comms seamlessly routed over simulated networks in EMANE or ns-3.

- **Technical Highlights:**
  - *Host fidelity*: Hosts are represented by VMs with relevant OS image and tactical applications
  - *Network fidelity*: High-fidelity network effects due to use of simulated network (EMANE and ns-3 models)
  - *Transparent forwarding* of VM traffic over simulated network
  - *Automated generation* of scenarios with specified vulnerabilities for wargaming exercises
  - *Realistic traffic* generated by synthetic users
  - *User Activity Tracker* tool captures data about user activities
  - *Comprehensive suite* of management tools

- **Multiple Deployments:**
  - Peraton Labs, Basking Ridge NJ
    - Remotely accessible by Government customers
  - Multiple Army labs
  - University/FFRDC partners

R. *Chadha et al., "CyberVAN: A Cyber Security Virtual Assured Network Testbed", IEEE MILCOM 2016.*

Relevant Past Work – A few examples

This paper describes the development of a belief system to model attackers' process of gathering information while interacting with a deceptive cyber defense system with the goal of quantifying the effectiveness of network deception.	Shridatt Sugrim, Sridhar Venkatesan, Jason Youzwak, Cho-Yu Jason Chiang, Ritu Chadha, Massimiliano Albanese and Hasan Cam, "*Measuring the Effectiveness of Network Deception*", Proc. of the 2018 IEEE Intelligence and Security Informatics (ISI), November 2018.
This paper describes VulnerVAN, a toolset that creates a vulnerable network scenario from a given spec in CyberVAN to realize an attack sequence. VulnerVAN also provides an attack blueprint that can guide a Red team or an automated attacker to execute the attack sequence. This capability is useful to support a large variety of defender-attacker studies.	Sridhar Venkatesan, Jason A. Youzwak, Shridatt Sugrim, Cho-Yu J. Chiang, Alexander Poylisher, Matthew Witkowski, Gary Walther, Michelle Wolberg, Ritu Chadha, E. Allison Newcomb, Blaine Hoffman, Norbou Buchler. "*VulnerVAN: A Vulnerable Network Generation Tool*", In Proceedings of IEEE MILCOM 2019, Norfolk, VA, 11–14 Nov. 2019.
This paper describes an Adaptive Cyber Deception System (ACyDS) that uses SDN reconfiguration capabilities to create deceptive network views to deceive attackers.	Cho-Yu Jason Chiang, Sridhar Venkatesan, Shridatt Sugrim, Ritu Chadha, Massimiliano Albanese and Hasan Cam, "*On Defensive Cyber Deception: A Case Study Using SDN*", IEEE MILCOM 2018, Oct 2018.
This paper describes an SDN-based reconnaissance system that thwarts network reconnaissance by delaying the scanning techniques of adversaries and invalidating their collected information, while minimizing the performance impact on benign network traffic.	S. Achleitner, T. F. La Porta, P. McDaniel, S. Sugrim, S.V. Krishnamurthy and R. Chadha, "*Deceiving Network Reconnaissance Using SDN-Based Virtual Topologies*," in *IEEE Transactions on Network and Service Management*, vol. 14, no. 4, pp. 1098-1112, Dec. 2017.
This paper describes the use of cognitive models as embedded computational agents for simulating human interactions with software and networks, and the use of cognitive models in the context of model-tracing for keeping track of human cognitive states to make better predictions of potential decisions and biases.	Vladislav Daniel Veksler, Norbou Buchler, Blaine E Hoffman, Daniel N Cassenti, Char Sample, Shridatt Sugrim, "*Simulations in Cybersecurity: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users*", Frontiers in Psychology - Section Cognitive Science, May 2018.
CyberVAN was used to support *Cyber Tatanka,* a 2-week cyber training event with over 100 participants hosted by the Nebraska Army National Guard. Peraton Labs designed vignettes and conducted training and red-teaming for the event.	KETV ABC. Nebraska National Guard troops and civilians train in joint cyberattack exercise. URL: https://www.ketv.com/article/guard-troops-civilians-train-joint-cyberattack-exercise/40450963

Peraton LABS

Contact us!

- We are looking to add strong partners to our team with strengths in:
  - Cyberpsychology-informed defenses and adaptation
  - Expertise in human cognitive bias modeling

Alexander Poylisher
Scientific Research/Analysis Senior Manager
apoylisher@peratonlabs.com

Ritu Chadha
Senior Research Director
rchadha@peratonlabs.com