CYBER RANGES

# Preparedness is Key to Deterrence

## OUR HISTORY IN BRIEF

Est. 2021, CYBER RANGES Corp. operates from Quantico Cyber Hub, Stafford VA, where we have deployed an on-premise cyber range together with the local SOC facility. CYBER RANGES has been a world-leading niche technology and system integration player in the global cyber security innovation market since 2014.

ISO 27001:2013 certified by the British Standards Institution (BSI), we effectively operate with multi-cultural teams (20+ nationalities) located in key locations for the international cybersecurity domain: Europe, the United Kingdom, Africa and North America. In GCC, India and East Asia we have also developed a formidable array of strong market partners.

The CYBER RANGES Advisory Board is currently chaired by Lt. General (Ret'd) Andrew Leslie, former Chief of Transformation for the Canadian Armed Forces.

Since 2018 our next-generation cyber range technology has officially powered the UN ITU's national, regional, and global cyberdrills. On April 19th, 2022 MITRE's commercial arm Engenuity announced an innovation partnership with us around CYBER RANGES Injector Engine and TOAR (Training Orchestration, Automation and Response) to develop and support the MITRE ATT&CK Defender 2.0 (MAD) and Purple Teaming initiatives.

MITRE ATT&CK Defender™

TOAR

We are an active research partner of the European Research Agency under Horizon 2020, a lead member of the European Cyber Security Organisation (ECSO), co-chairing WG5 on cyber ranges, education and training, and technical exercises. We also work closely with the Global Cyber Alliance (GCA, in New York, London, Brussels) in its mission to fight cyber crime. We have delivered focused, ground-breaking projects for DCAF and USAID in the Balkans.

> "By 2024 a cyberattack will so damage critical infrastructure that a member of the G20 will reciprocate with a declared physical attack"
>
> GARTNER
> Top Cybersecurity Predictions

**Lt. General (Ret'd)**
**Hon. Andrew Lesley**
Chairman, Advisory Board

**Dr. Al Graziano**
Chief Executive Officer

# Our Mission & Objectives

**CYBERSPACE HAS BECOME CRITICAL** for the conduct of modern military and law-enforcement activities and is recognized as the new global theatre of operations. While land, sea, air and space are the prevailing environments of operations, there has been a growing need to engage in and operationalize cyberspace.

Army futures and law-enforcement force modernization priorities place great importance on integrating wireless communications, digital displays, and an ever-growing number of sensors to gather, disseminate, and exploit growing data sets to maintain information superiority and full-spectrum dominance.

> *In a contested battlefield, blue force tracking, spatial awareness, and effective communications between friendly units remain vitally important*

Tracking enemy combatants across complex and degraded environments and protecting networks through robust cyber security continue to be key to guaranteeing mission success.

In light of the complex and rapidly evolving nature of the cyber domain, Military and Law-Enforcement entities recognize the need for robust cyber capabilities to ensure mission success.

CYBER RANGES provides a highly scalable TOAR-enabled Persistent Cyber Training Environment (PCTE), to develop cyber war fighters in tactics, techniques and procedures for offensive and defensive operations.

Traditional cyber range implementations have so far operated independently of the traditional kinetic mission training programmes for the conventional battle personnel. As a result, cyber mission forces have often trained only on the cyber elements of a campaign.

CYBER RANGES provides for the rapid implementation of complex and competitive cyber exercises for training SecOps and critical network defence personnel in a safe, simulated environment.

> *Cyberspace has become critical for the conduct of modern military and law-enforcement action*

# Our Technology and Services

**CYBER RANGES PROVIDES** a secure, isolated testing environment closely emulating a client's unique computer and network infrastructure so that exercises can safely include both attack and defence factors, as well as system security controls. CYBER RANGES can create multiple testing environments with hundreds or thousands of virtual machines in just hours, when each used to take days or even weeks to build.

CYBER RANGES is a military-grade cyber-ranging platform that can be used by both individual active-duty operations personnel and command organizations to practice cyber security skills and capability in a "hands on" and challenging way.

In addition to hosting cyber and tabletop exercises, CYBER RANGES serves as an educational and research environment to develop and master the latest tools, defences and other techniques to protect systems and networks from cyber attackers. Customers can better and more securely plan large-scale changes to their infrastructure by first testing them in an emulated environment for stability, scale and security.

Cyber Forces are those military and civilian personnel that force generate, force employ and force develop Cyber Operations, Network Operations and Cyber Mission Assurance. At CYBER RANGES we can address the technology and content of required Training Programmes to develop mission-ready Cyber Forces through collective or individual learning, training and practice.

Cyber preparedness levels are becoming increasingly important as the demand for cyber activities continues to grow, indicating future readiness challenges. Standards need defining before personnel qualifications are established or vice versa. We propose, as equally important, to ensure that cyber components are integrated in Force Posture & Readiness (FP&R).

← CONTINUED FROM PAGE 3

*Creating realism in a sandbox test environment isolated from the operational environment is a special challenge in cyberspace*

The CYBER RANGES design combines gamification principles with interactive challenges to test mission-critical cyber security competence across a wide range of domains, either individually or in a team against others.

CYBER RANGES provides a unique environment for cyber security testing throughout the program development life cycle using unique methods to assess resiliency to advanced cyberspace security threats.

Replicating the scale and diversity of the complex C5ISR communication networks at such high fidelity to realistically portray current and anticipated attack strategies (e.g., Malware, Distributed Denial of Service attacks, Cross-Site Scripting) is a complex task.

CYBER RANGES addresses this challenge by replicating IT / OT environments by employing a multitude of virtual machines and physical hardware (as required) augmented with use traffic and attack emulation, port / protocol / service vulnerability scanning, and data capture tools. Coupled with a structured test methodology, Command observers can efficiently and effectively engage with the cyber-ranging facility (on-site, online, transportable) to gain cyberspace resiliency insights.

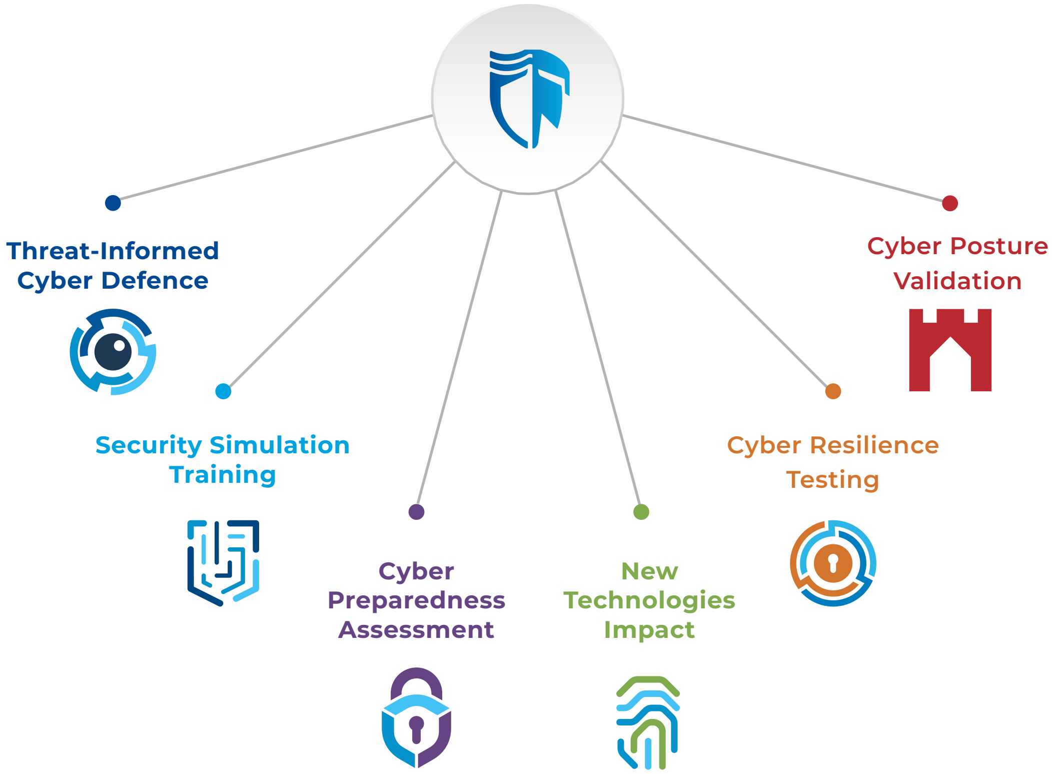
When applied, the CYBER RANGES capability allows Military / Law-Enforcement entities to incorporate cyber security early in any project implementation, thus avoiding high-cost integration at the end of the development life cycle.

CYBER RANGES is the next-generation cyber range for the development of cybersecurity skills and the validation of cyber capability and organizational resilience. CYBER RANGES harnesses the power of cloud technology to manage the entire management lifecycle of high-fidelity deep-dive scenarios, from their creation to their distribution and delivery to end users, meeting even the most demanding use cases of a cyber range today. CYBER RANGES can integrate 3rd-party vendor controls.

CYBER RANGES is available as a cloud-based solution, or it can be deployed on- premise to scale for the support of thousands of virtual machines. Thanks to its flexibility, CYBER RANGES is used today by government, military, academia, and businesses around the world.

Through its powerful Injector Engine, CYBER RANGES can simulate both benign and malicious traffic, complex cyberattack flows, and user activities making CYBER RANGES the turnkey solution for the delivery of hands-on exercises, blue team exercises, red team exercises and war gaming exercises.

# The cyber range of choice for threat-informed defenders



Threat-Informed Cyber Defence

Security Simulation Training

Cyber Preparedness Assessment

New Technologies Impact

Cyber Resilience Testing

Cyber Posture Validation

| CYBER RANGES Use Cases | | CYBER RANGES Features |
|---|---|---|
| Threat-informed Cyber Defence | 1 | Next-Generation Cyber Range Technology |
| Deep-dive Situational Experiences | 2 | TOAR-enabled |
| Individual and Team-based Practice | 3 | Range “on Tap”, Managed, On-Prem, Portable |
| Self-paced, Instructor-led, Anywhere Anytime | 4 | Transportable Command Center |
| Learning Pathways on multiple criteria | 5 | Complex Threat Emulation Scenarios |
| Top 10 Abilities | 6 | Virtual IT/OT/ICS/IoT Infrastructures |
| Talent Selection and On-Boarding | 7 | Off-the-shelf, Bespoke, Drag-n-Drop Replication |
| Table-Top Crisis Simulations, Cyber and Cross Cyber Exercises | 8 | Advanced Injector Engine for Use Traffic and Attack Emulations |
| CTFs, Regional Competitions, SOCathons | 9 | Full Support of MITRE ATT&CK® |
| Transitioning from active service | 10 | Bring Your Own Device (BYOD) |
| Cyber War Games, LiveFIRE eXperiential Courses (APT editions) | 11 | Third-Party Controls Integration, e.g., SIEM, WAF, EDR, XDR, NGFW, etc. |
| Blue v Red Team, DevOps, White Team Drills | 12 | Integration with LMS and HCMS |
| Product Testing, Proof-of-Value | 13 | Start-to-finish performance metrics |
| Integration with SOC, Cyber Defence Centers, C5ISR | 14 | Competency Frameworks, e.g., NIST NICE and bespoke |
| Portable Command Center for in-theatre support of kinetics and command post exercises | 15 | CYBER RANGES OT WORLDS for ICS, SCADA, IoT hybrid simulations |

# Bringing access to Performance Advances at the Point-of-Need

> *CYBER RANGES delivers "training as-a-service" and its mobile deployments effectively bring deep-dive training to the point-of-need*

**CYBER RANGES PORTABLE** and CYBER RANGES COMMAND CENTER offer a compact, rugged implementation of CYBER RANGES cloud technology to enable interoperable, mobile options for deep-dive simulation learning and training directly in the field.

Increased flexibility is an essential driver in the spectrum of training and simulation initiatives across the armed forces – including the US Army's Synthetic Training Environment (STE), or the programs from the Naval Air Warfare Center Training Systems Division.

CYBER RANGES PORTABLE presents the smallest system footprint available on the market, without sacrificing the high-end automation and orchestration performances of its larger on-cloud and on-prem deployments.

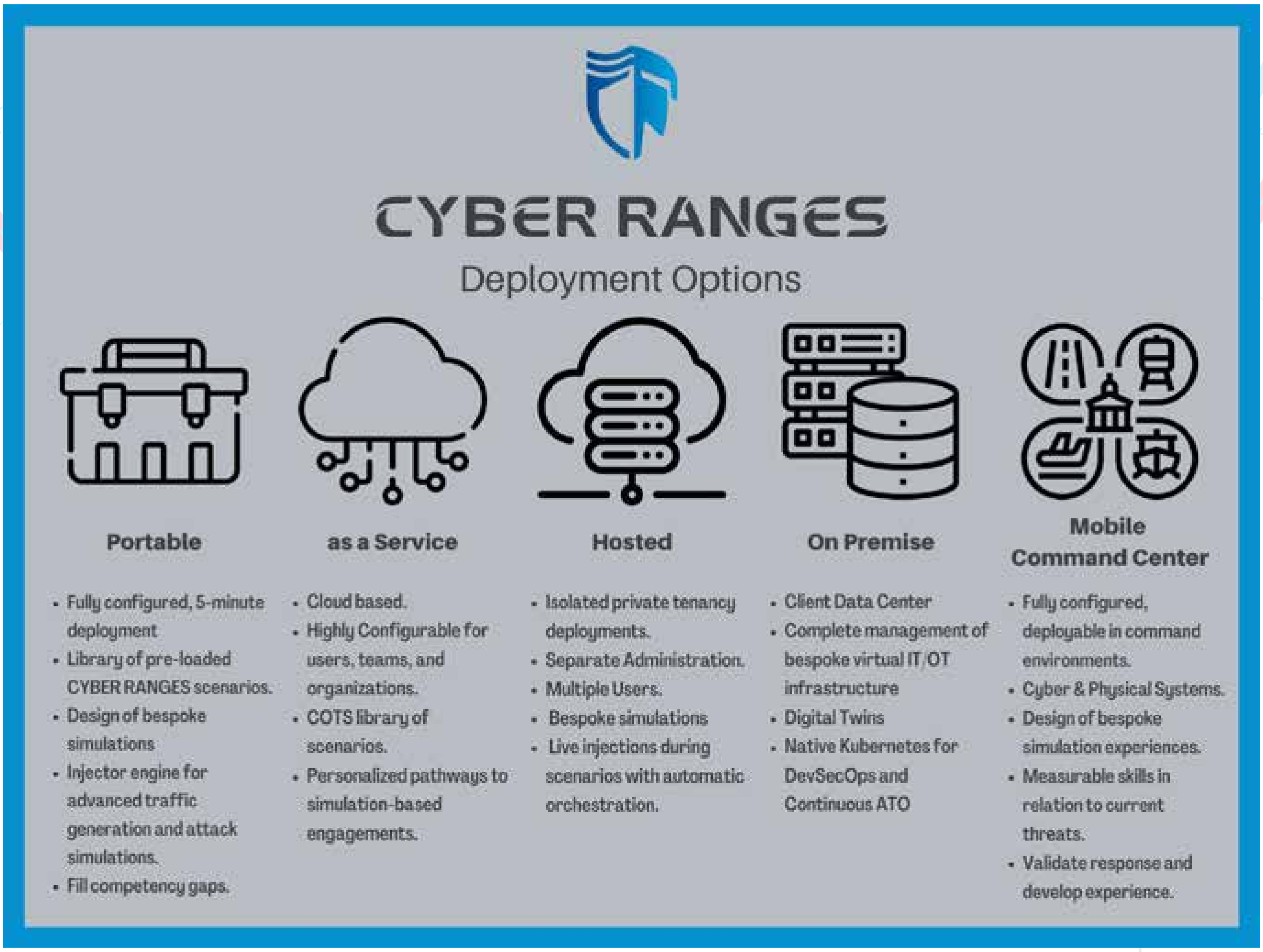
CYBER RANGES delivers highly flexible and scalable training capabilities increasing mission readiness for soldier, sailor, airman, or Marine, no matter the environment or geographic location.

Our cloud technology enables interoperable, mobile options for deep-dive simulation training directly in the field

CYBER RANGES advances crucial capabilities through high-performance cyber situational experiences. CYBER RANGES PORTABLE and CYBER RANGES COMMAND CENTER are capable of connecting multiple simulation devices to a single, centralized environment without slowing performance, even while scaling to accommodate varying requirements for numerous users.

CYBER RANGES brings together the advantages of on-cloud and on-premise deep-dive simulation training into powerful, in-threatre, secure, hybrid range-to-users environments.

CYBER RANGES Scenario Composer and Injector Engine allow field instructors to design and fine-tune simulation scenarios at the point-of-need. This is particularly important when in-theatre kinetic performance is integral part of an overall cyber-physical simulation exercise.



# CYBER RANGES

## Deployment Options

### Portable

- Fully configured, 5-minute deployment
- Library of pre-loaded CYBER RANGES scenarios.
- Design of bespoke simulations
- Injector engine for advanced traffic generation and attack simulations.
- Fill competency gaps.

### as a Service

- Cloud based.
- Highly Configurable for users, teams, and organizations.
- COTS library of scenarios.
- Personalized pathways to simulation-based engagements.

### Hosted

- Isolated private tenancy deployments.
- Separate Administration.
- Multiple Users.
- Bespoke simulations
- Live injections during scenarios with automatic orchestration.

### On Premise

- Client Data Center
- Complete management of bespoke virtual IT/OT infrastructure
- Digital Twins
- Native Kubernetes for DevSecOps and Continuous ATO

### Mobile Command Center

- Fully configured, deployable in command environments.
- Cyber & Physical Systems.
- Design of bespoke simulation experiences.
- Measurable skills in relation to current threats.
- Validate response and develop experience.

CYBER RANGES

CYBER SPACE, ENGAGED.

Call us in North America toll-free

**1-800-959-0163**

CYBER RANGES Corp.
Quantico Cyber Hub
Suite 305, 1010 Corporate Drive
Stafford, VA 22554

contact@cyberranges.com

www.cyberranges.com