



ADVANCED CYBER SECURITY CENTER

COLLABORATIVE DEFENSE • TRUSTED NETWORKS



Pending inclusion of poll results
(not sure where to put them in terms of the flow)

Cyber ranges and exercises

Continuous assessment of talent, teams and tools

October 21, 2021

11th ANNUAL CONFERENCE: *Integrated strategies for cyber talent and technology*

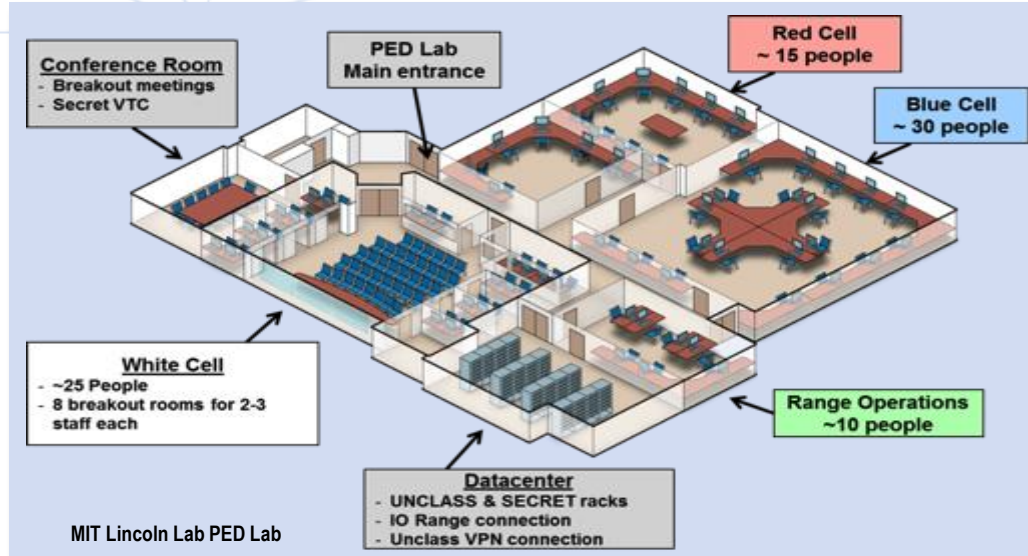
What is a cyber range?

A virtual environment used for cyber training, software development and testing

ACSC is running three cyber range exercises this year with seven of our lead partner organizations



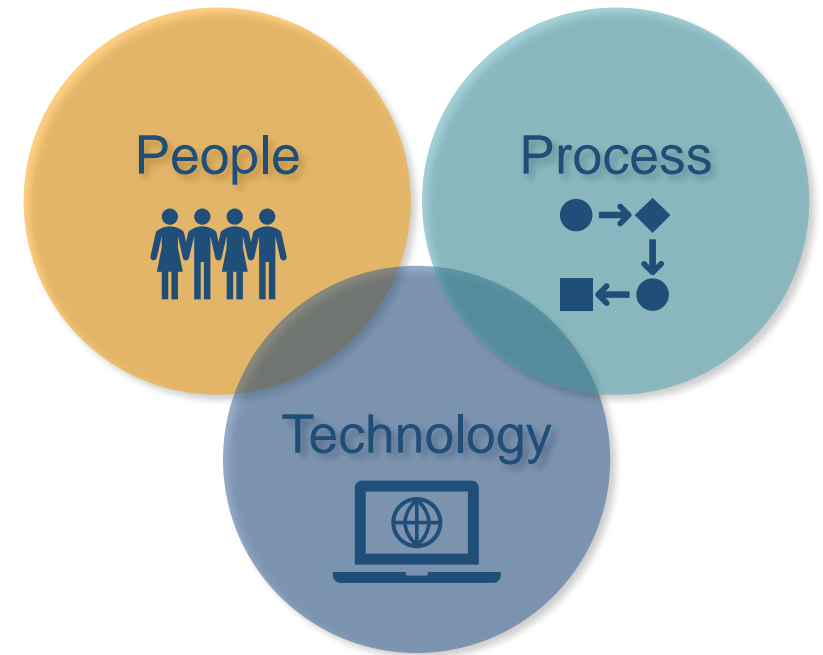
Example: Cyber Red/Blue exercises for assessing DoD Cyber Protection teams



What's the issue?

- **People:** Limited use of sophisticated platforms and practices to train and develop cybersecurity defender teams in realistic environments
- **Process:** Still too many barriers preventing partnerships within and across organizations and between the public and private sector
- **Technology:** Untapped opportunity to assess new technology tools efficiently and realistically using sophisticated platforms that align to internal environments

All these challenges lend themselves to collaboration that will accelerate solutions, reduce costs and improve security



Range-based exercises accelerate innovation, reduce cost and improve security

Current Practice

- Non-technical tabletop exercises – low technical fidelity
- Single enterprise, no outside collaboration
- Limited range marketplace and vendor-specific platforms to assess tools
- Few opportunities to develop and assess front-line defensive teams

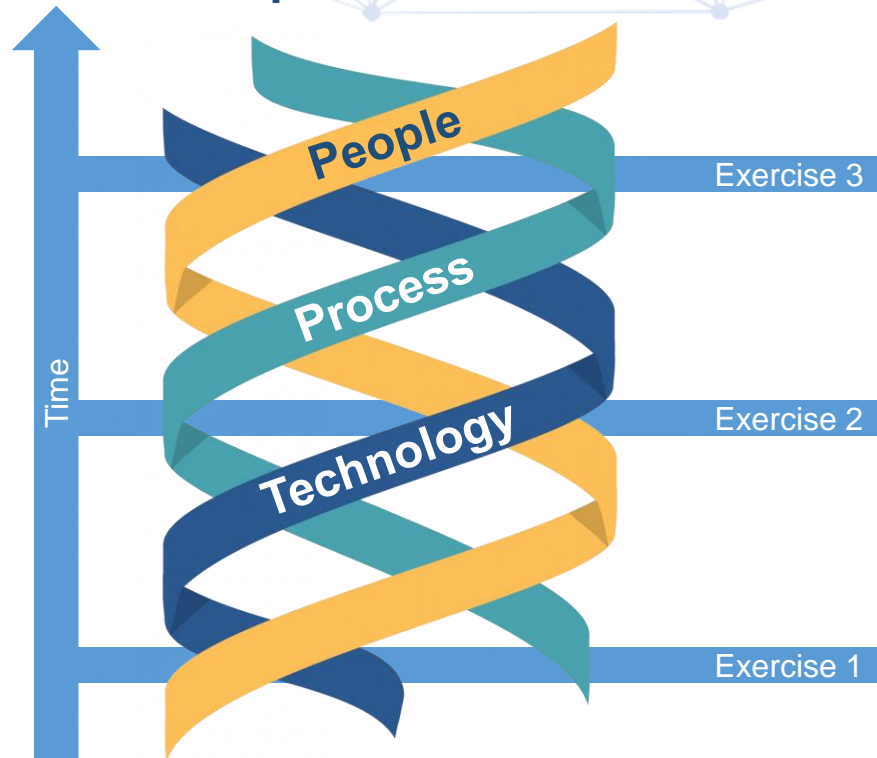
Emerging Practice

- Range-based training exercises – high technical fidelity – well-suited to emerging cloud environments
- Multiple, collaborating enterprises, including state and federal government
- Data-driven tool acquisition, integration, assessment
- Significant value at all levels of the enterprise



Cyber exercises provide significant impact over time

Triple Helix Model *



Exercises on ranges provide an opportunity to develop and assess the continuous evolution of people, process and technology

**Adapted from US Defense Advanced Research Projects Agency (DARPA), e.g., <https://pal.sri.com/wp-content/uploads/publications/calio/2009/1746.pdf>*



Emerging model: Developing and assessing SOC staff with metrics and range exercises

Major bank

Identify individual & team gaps with data

Mentorship program & training

Individual exercise opportunities

Cyber range team exercises

Reassess and identify new gaps

Framed around a career path for cybersecurity analysts and architects



The ACSC opportunity for collaborative defense

Cyber ranges in action

	Parallel play teams	Joint teams
People	<ul style="list-style-type: none">• Individual exercises highlight gaps, track progress and provide peer benchmarks• Shared takeaways across organizations	<ul style="list-style-type: none">• Staffs learn from peer organizations• Build peer networks across organizations
Process	<ul style="list-style-type: none">• Internal collaboration across technical and business functions in an organization• External collaboration across private and public sectors	
Technology	<ul style="list-style-type: none">• Assess new technologies and innovative tools in a secure environment through collaborative sandboxes• Accelerate innovation and reduce costs	



Advanced Cyber Security Center

Mission:

Collaborative Defense

The region's only non-profit, member-driven, cross-sector organization operating under an NDA and committed to strengthening member cybersecurity defenses, building effective collaboration with the public sector, and preparing the region's response to large scale cyber threats.

The ACSC is uniquely positioned to ensure our members and the region are national leaders in "Collaborative Defense."



Member organizations and leaders

Abacus Insights – Bill Brown

Brandeis University – David Albrecht

Founding Member & Lead Partner:

Commonwealth of Massachusetts – John Merto

Founding Member & Lead Partner:

Dell Technologies

Everbridge – Sonia Arista

Foley Hoag

Founding Member & Lead Partner:

Federal Reserve Bank of Boston – Anjan Bagchee

Foundation Medicine – Robert Marcotte

Harvard University – Nathan Hall (acting)

Founding Member & Lead Partner:

Liberty Mutual – Katie Jenkins

Founding Member & Lead Partner:

Manulife/John Hancock – Tom Laroche & Greg Thompson

Lead Partner:

MassMutual – Ariel Weintraub

Mimecast – Neil Clauson

Founding Member:

MIT Lincoln Laboratory – Brian McCarthy

Founding Member:

MITRE Corporation – Mick Costa

Lead Partner:

MunichRe – John Schramm & Greg Brinkman

Northeastern University – Harry Hoffman

Point32 Health – Mark Teehan

Lead Partner:

PTC – Eric Hussey

Rapid7 – Tas Giakouminakis

Lead Partner:

Schneider Electric – Patrick Ford

Founding Member & Lead Partner:

State Street Corporation – Liz Joyce

Veracode – Sohail Iqbal

VHB – Greg Bosworth

VMware Carbon Black – Chris Weldon



Thank you!

Co-chairs



Patrick Ford
CISO for Americas region
Schneider Electric



Katie Jenkins
EVP & CISO
Liberty Mutual
ACSC Board Member



Marc Zissman
Associate Head, Cyber Security & Information Sciences Division
MIT Lincoln Laboratory
ACSC Board Member

Research Partner Presenters



Paul Winter
Director of Professional Services
SimSpace



David Berliner
Director of Product
SimSpace

Leading Practitioners



Jeff Fisher
Director, Cyber Range Platforms
US Department of Defense



Athie Self
Vice President Global Technology
Project Manager
JP Morgan Chase & Co

Expert Resources

Dan MacDonnell
Chief Strategy Officer
Randori

Bill Brown
Chief Information Security Officer & CIO
Abacus Insights

Matt McHugh
Director of Information Security, Risk & Compliance
Federal Reserve Bank of Boston



Thank you to our 2021 conference research partners...



...and our conference sponsors

