CYBER RANGES

Train as You Fight, Fight as you Train

November 2014

ROMANIA

THE CYBER SECURITY FORUM INITIATIVE

Guvernul României

Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică

Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013.

Hotărâre pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică

The best way to fully understand the weakness present in a network is to attack a network. This is called “penetration testing” or “ethical hacking”

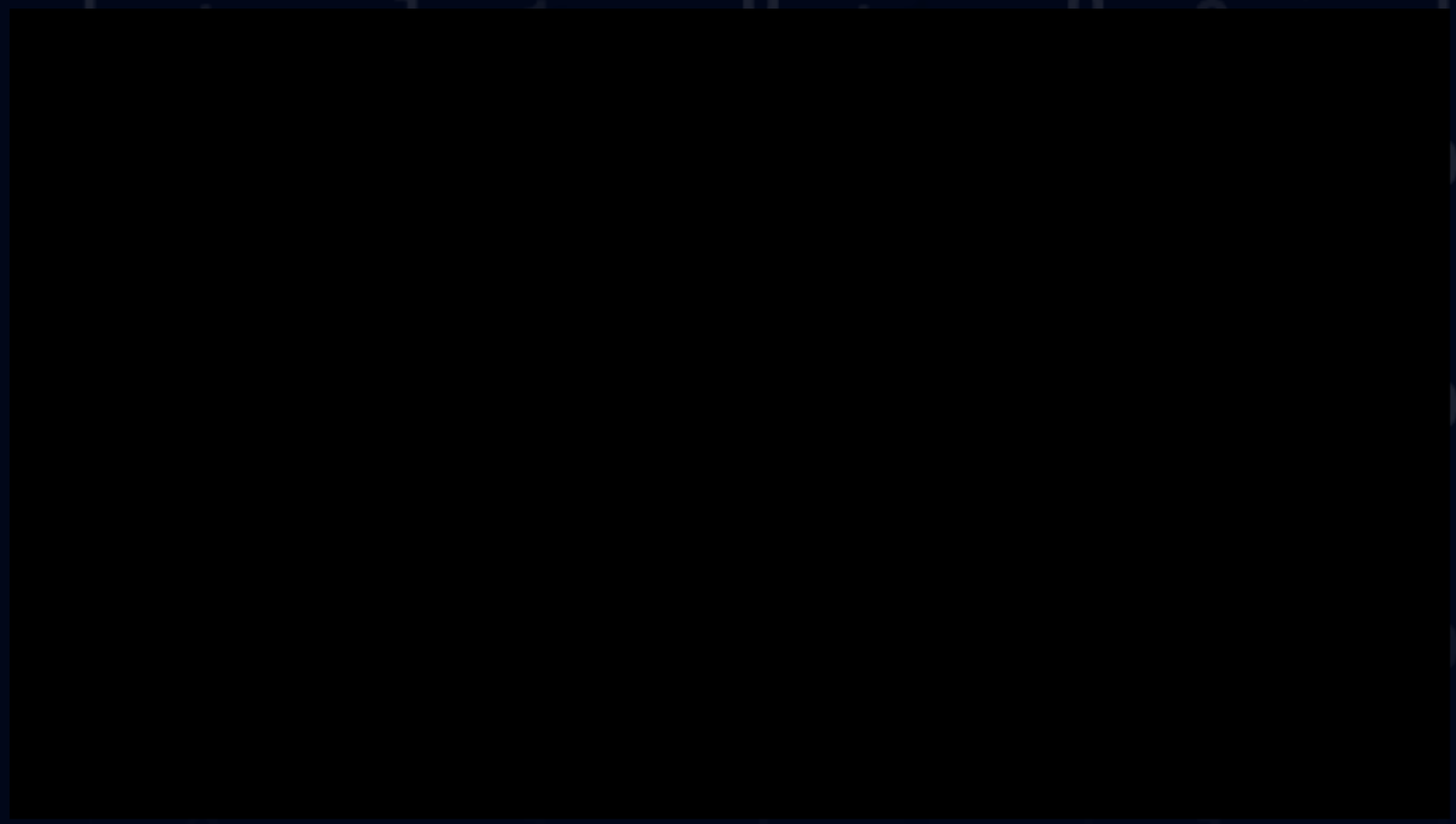
How do we do that?

Cyber Range

What are the challenges?

Time - Scale - Cost

Cyber Range - Michigan Effort
Hybrid Approach

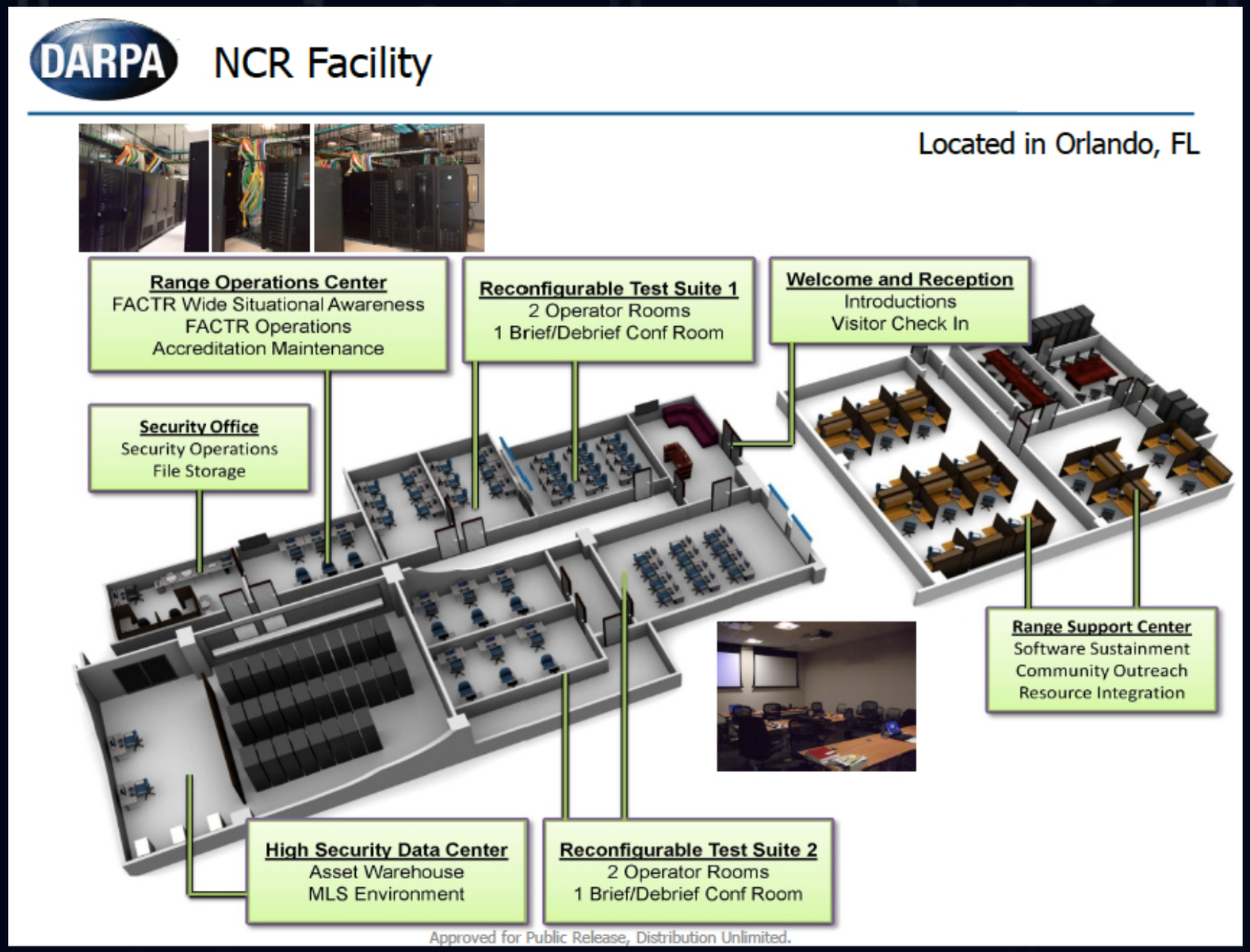


DoD Cyber Range Strategy - Gov Only

"The development of the National Cyber Range will enable the success of these and other efforts, allowing DoD, other U.S. government entities, and potentially non-U.S. government partners to test and evaluate new cyberspace concepts, policies, and technologies."

http://www.defense.gov/news/d20110714cyber.pdf

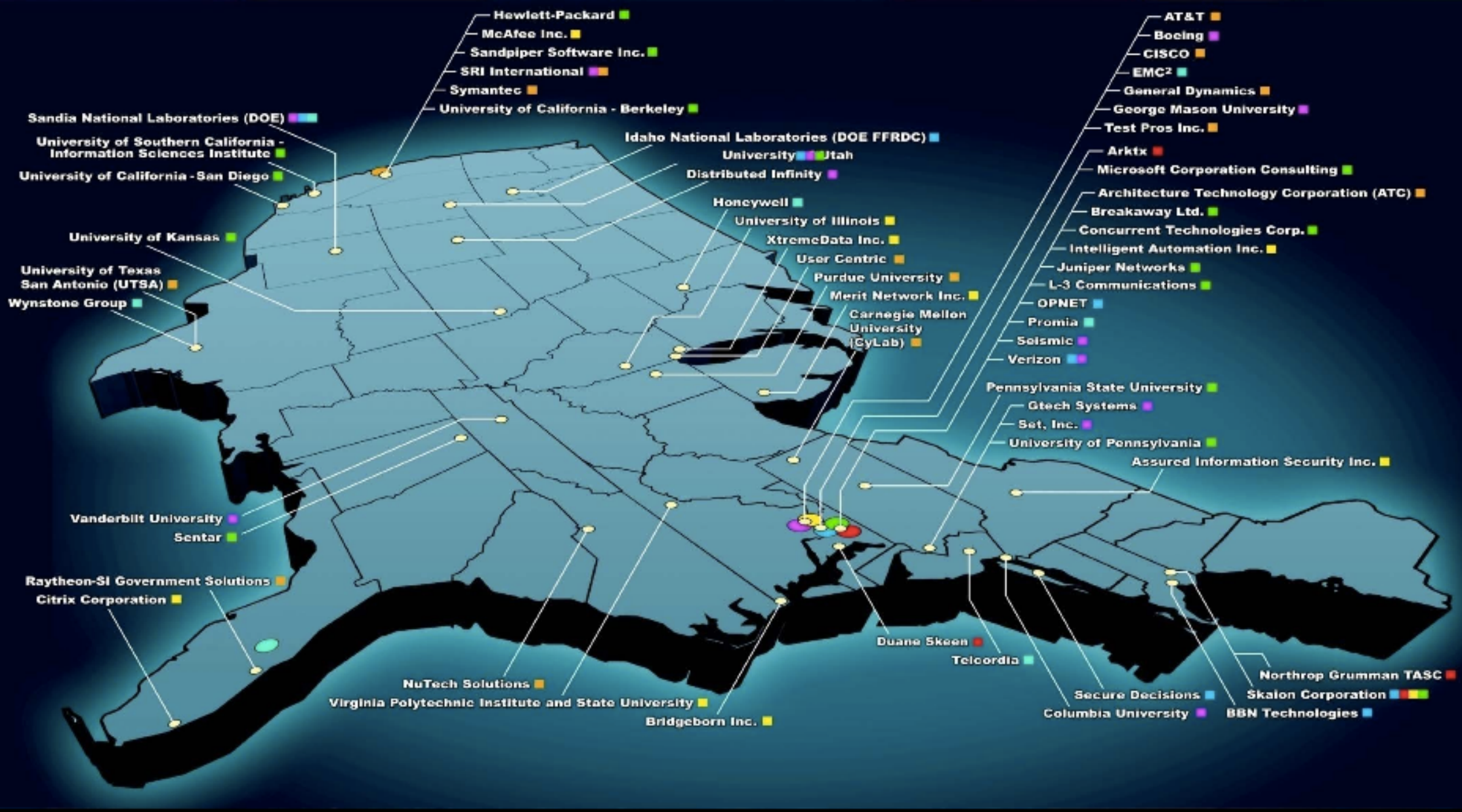
US National Cyber Range (NCR)



Multilevel security or **multiple levels of security** (**MLS**) is the application of a computer system to process information with **incompatible classifications** (i.e., at different security levels), permit access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization.

NCR Team

BAE SYSTEMS | GENERAL DYNAMICS | APL (Johns Hopkins University Applied Physics Laboratory) | LOCKHEED MARTIN | NORTHROP GRUMMAN Information Technology | SAIC From Science to Solutions | SPARTA A Subsidiary of Cobham



Providing the environment to solve the Nation's Cyber problems

UNCLASSIFIED: Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)

CERT® EXERCISE NETWORK (XNET) - restricted

XNET supports force-on-force (Red Team/Blue Team) scenarios. Attacks can be scripted or conducted by a connected live aggressor force.

What is a Cyber Range? (In a nutshell)

A scale model of the Internet (Internet in a box)

Used to carry out Cyber War Games - Blue x Red

Creates access to realistic, hands-on Cyber Security Training scenarios

Used to test new technologies
Simplified ability to introduce, execute, and test new (malicious) code

Popular Cyber Ranges - Commercial

- DEFCON - Built from scratch every time. Once a year hands-on training.
- SAIC Cyber Patriot, L3 NSS (DCOE), Sypris, Mile2, ThreatSPACE® Live-Fire, SANs NetWars CyberCity, CTF365 (Romania),

Train as You Fight, Fight as you Train

Be OPERATIONAL in Cyberspace!

What Are Cyber Warriors?

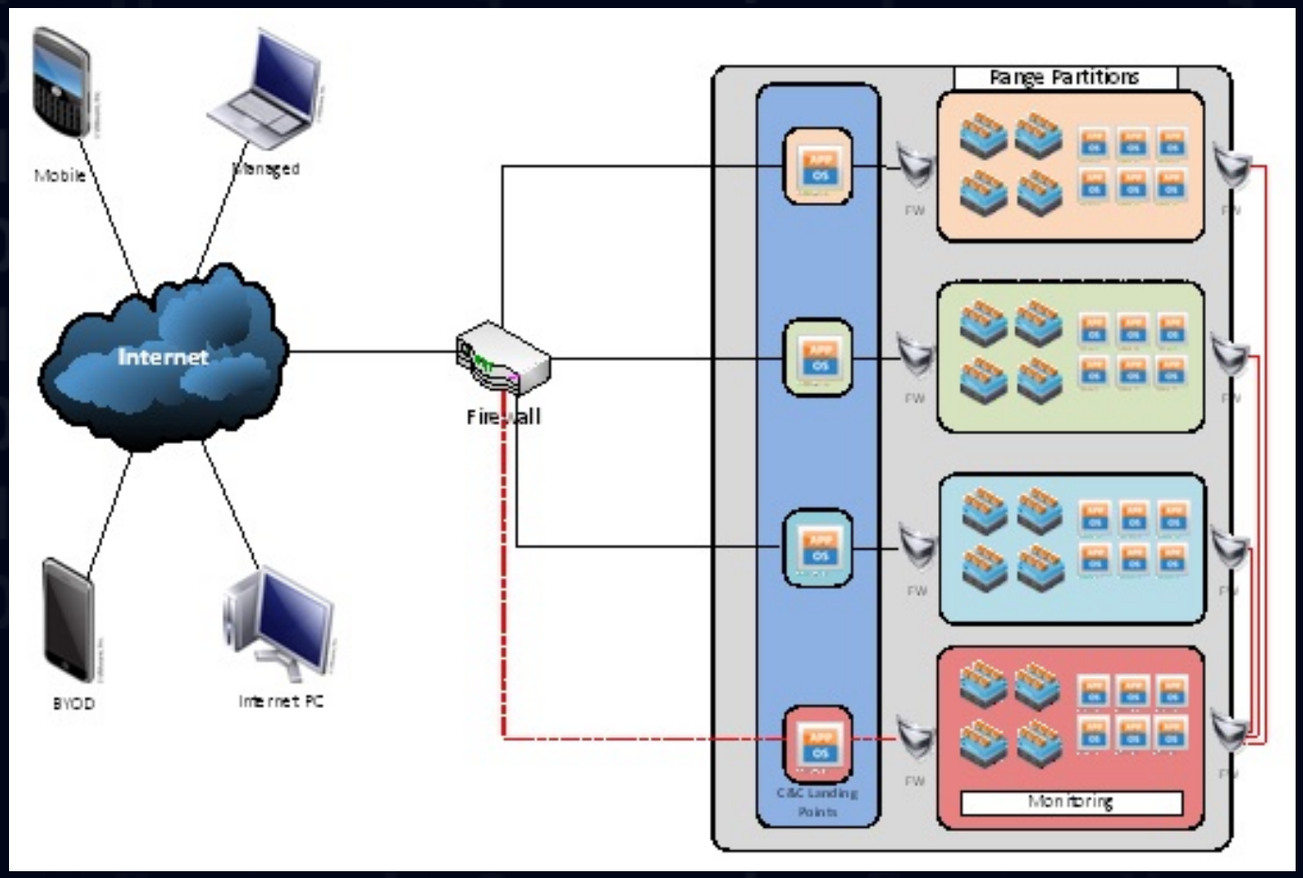
US Army Gen Keith Alexander, cyber warriors are a skilled force **capable of full-spectrum cyber operations** across a continuum of threats" (Alexander vows that DOD will have full cyber readiness by 2014, Defense Systems Jul 17 2012)

CSFI training and L3 NSS Training

Provides isolated Host enclave environments, offering multiple enclaves for different Students

Provides “hardware-in-the-loop” (HIL) simulated device (Cisco WAP), other devices

Simulated protection systems such as HIDs



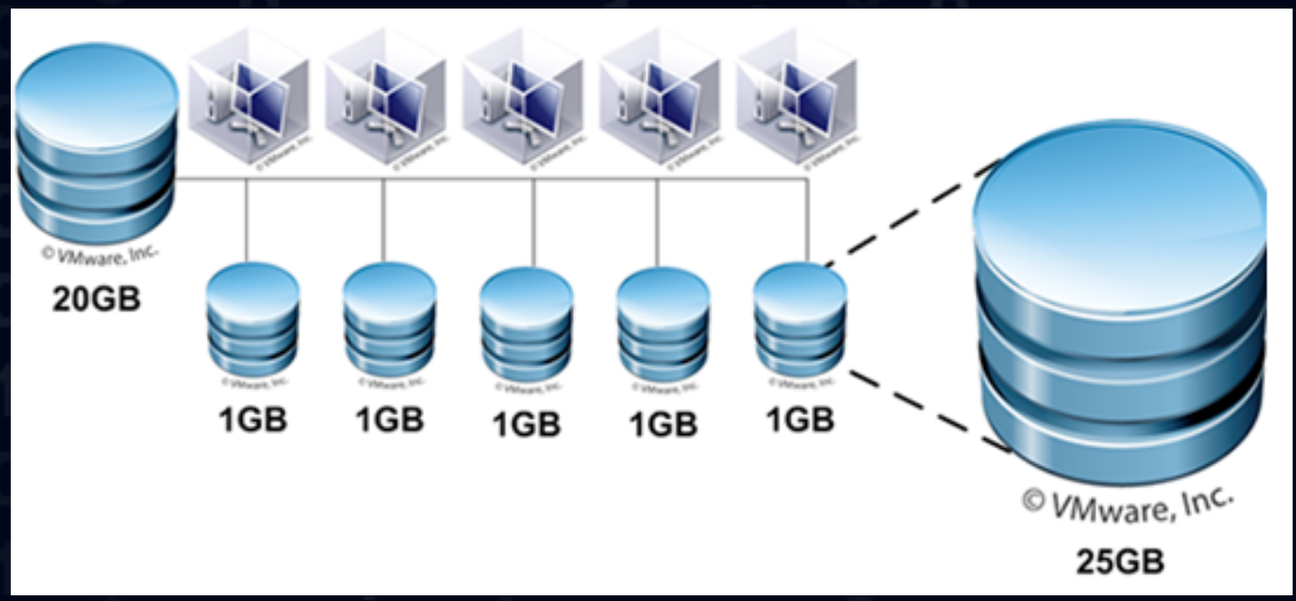
Source: Provided by L3 NSS

Rapid Provisioning

Custom vApps can be created on demand (Active Directory, Linux etc.)

Custom Distros Such as FoxOp Cyber security tool kit and Kali Linux

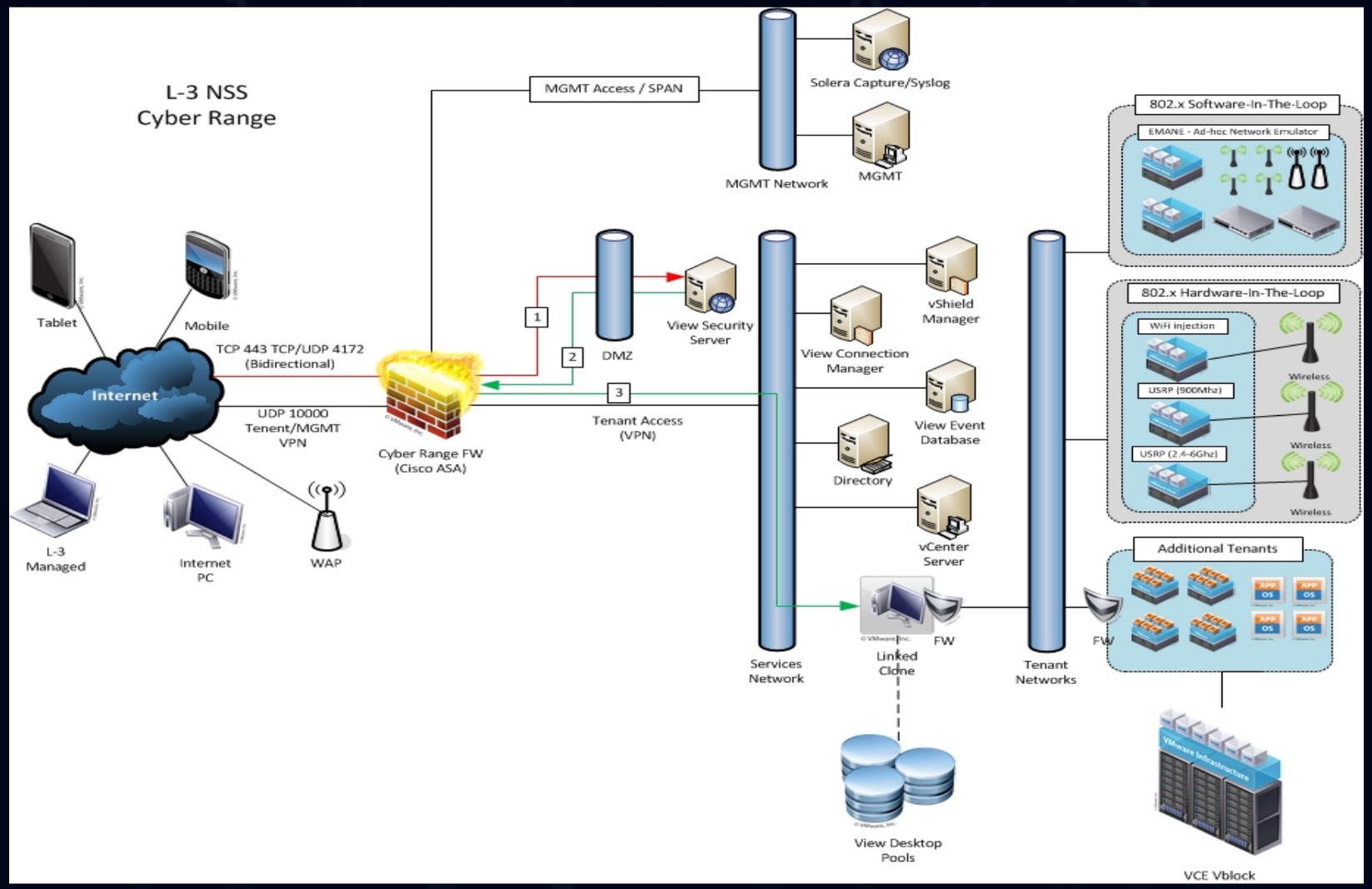
Resources can be dynamically allocated and removed as requirements change



Source: Provided by L3 NSS

VM L3 CSFI Cyber Range Example

- Firewalls
- Routers
- Target Servers
- Wireless simulators
- DNS Servers
- Databases



Source: Provided by L3 NSS

Custom Tools used by CSFI in the Cyber Range

Pre-Loaded and Pre-Configured with Key Cyber Security Tools

Featuring **40+** of the industry's leading, most used, and some of the most difficult to configure open source tools all on one Distro

All tools on the USB are pre-configured and highly integrated for immediate plug-n-play, out-of-the-box ease of use and speed

Customized for use through FOXOP's proprietary OSSEC dashboard and with FOXOP's Integrated Situational Awareness panel

Channeled through Procysive's Honeynet of 13 international servers

Featuring 10 proprietary tools

Configured on a Linux-based platform leaving zero footprint on host computer

1024-bit twisted encryption SSH and instant VPN tunnel to Secure Phone, browser, video, and IRC

Obfuscation capabilities, DNS rotation, and fully functional IDS

FOXOP/CSFI Main C2 (Command and Control) on L3 Cyber Range

Takeaways

Cyber Range is a powerful training tool

Cyber Range can be used to boost national security

Cyber Range emulates reality without compromising users and systems

Cyber Range is a great R&D development platform

contact@csfi.us

www.csfi.us