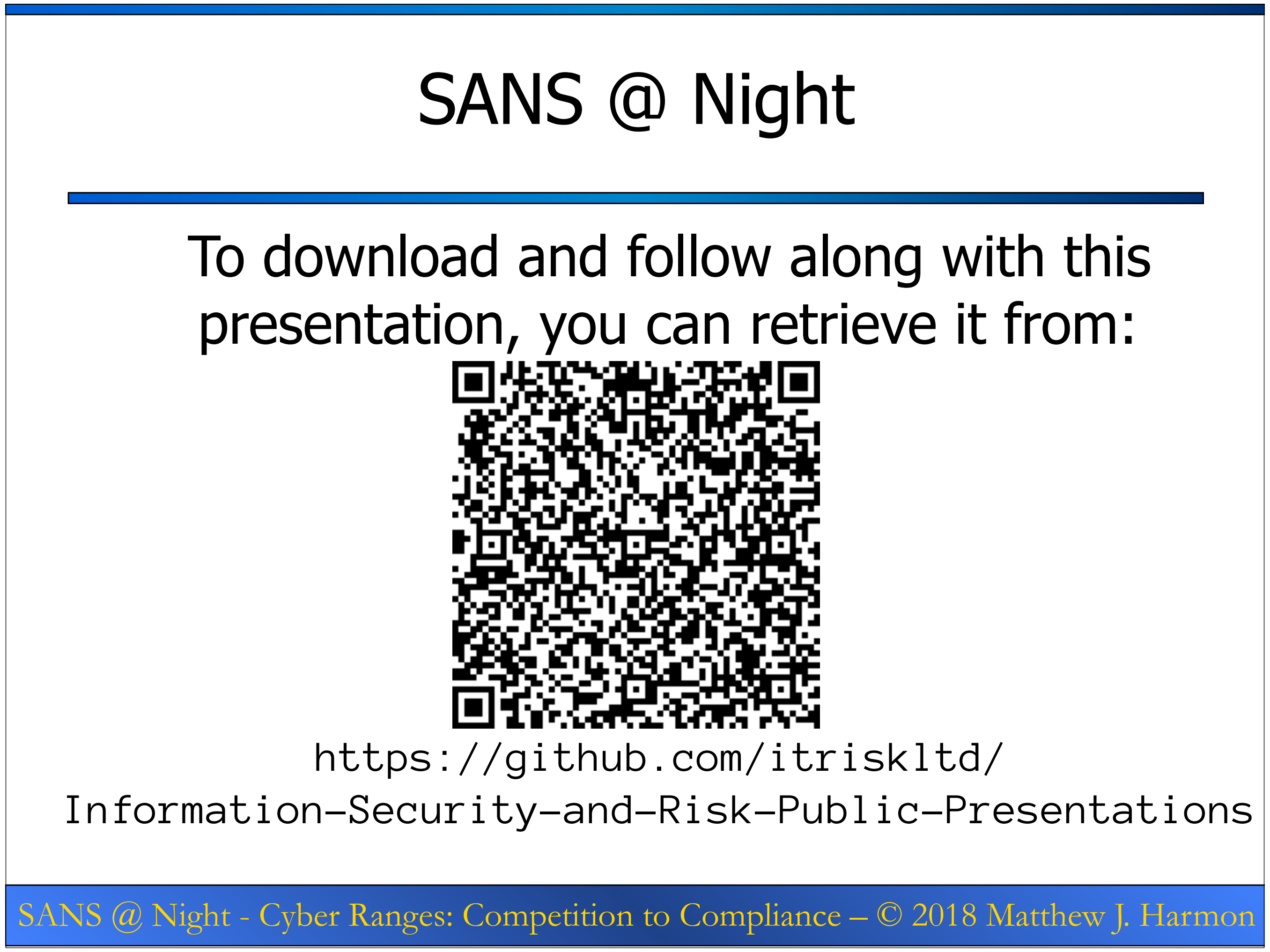
Boomer the Bangle Boarding

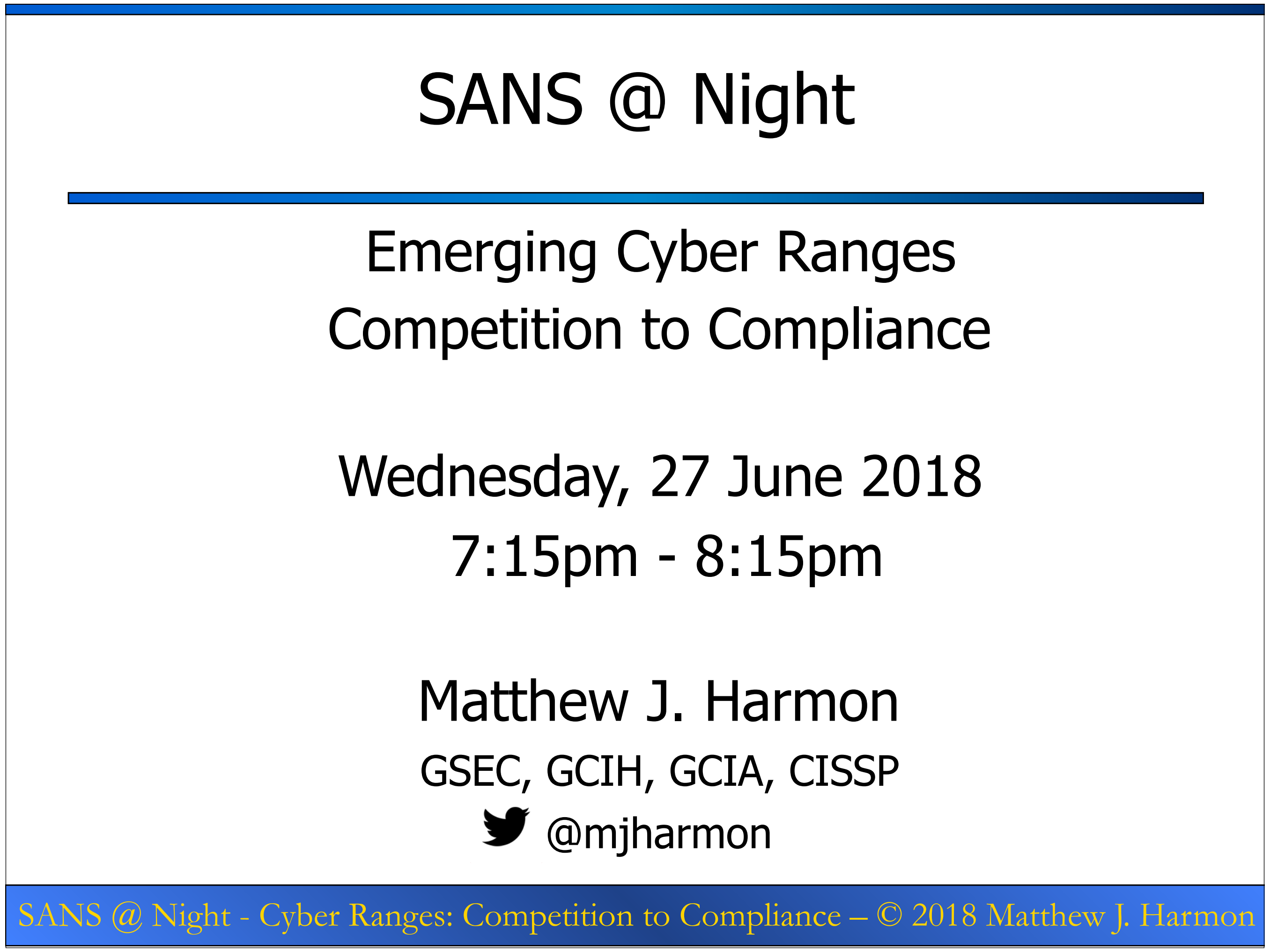


SANS @ Night

To download and follow along with this presentation, you can retrieve it from:

https://github.com/itriskltd/Information-Security-and-Risk-Public-Presentations

I've pre-released tonights presentation, you can pick up a PDF with that QR Code or enter in the GitHub link.



SANS @ Night

Emerging Cyber Ranges
Competition to Compliance

Wednesday, 27 June 2018

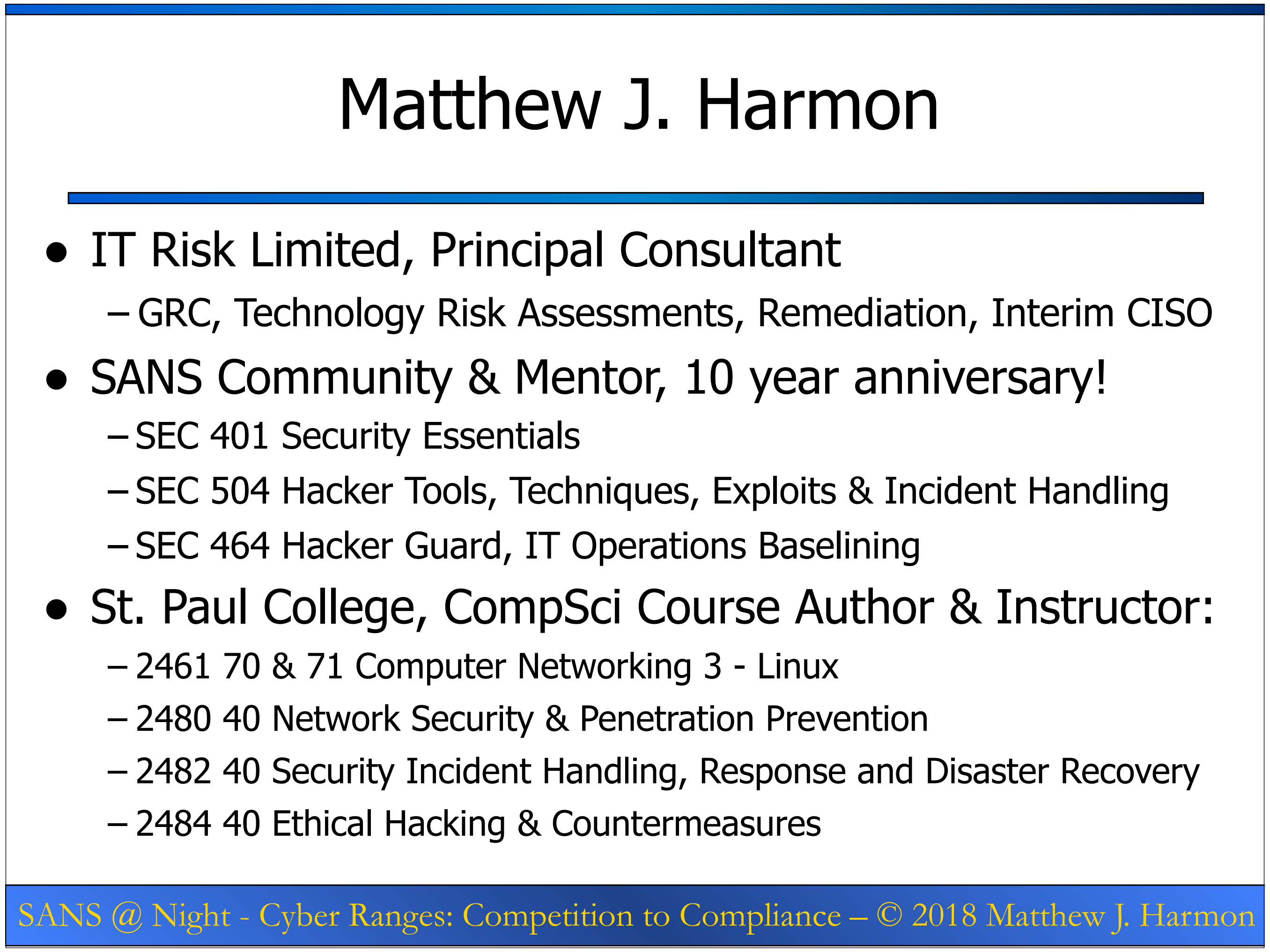
7:15pm - 8:15pm

Matthew J. Harmon

GSEC, GCIH, GCIA, CISSP

@mjharmon

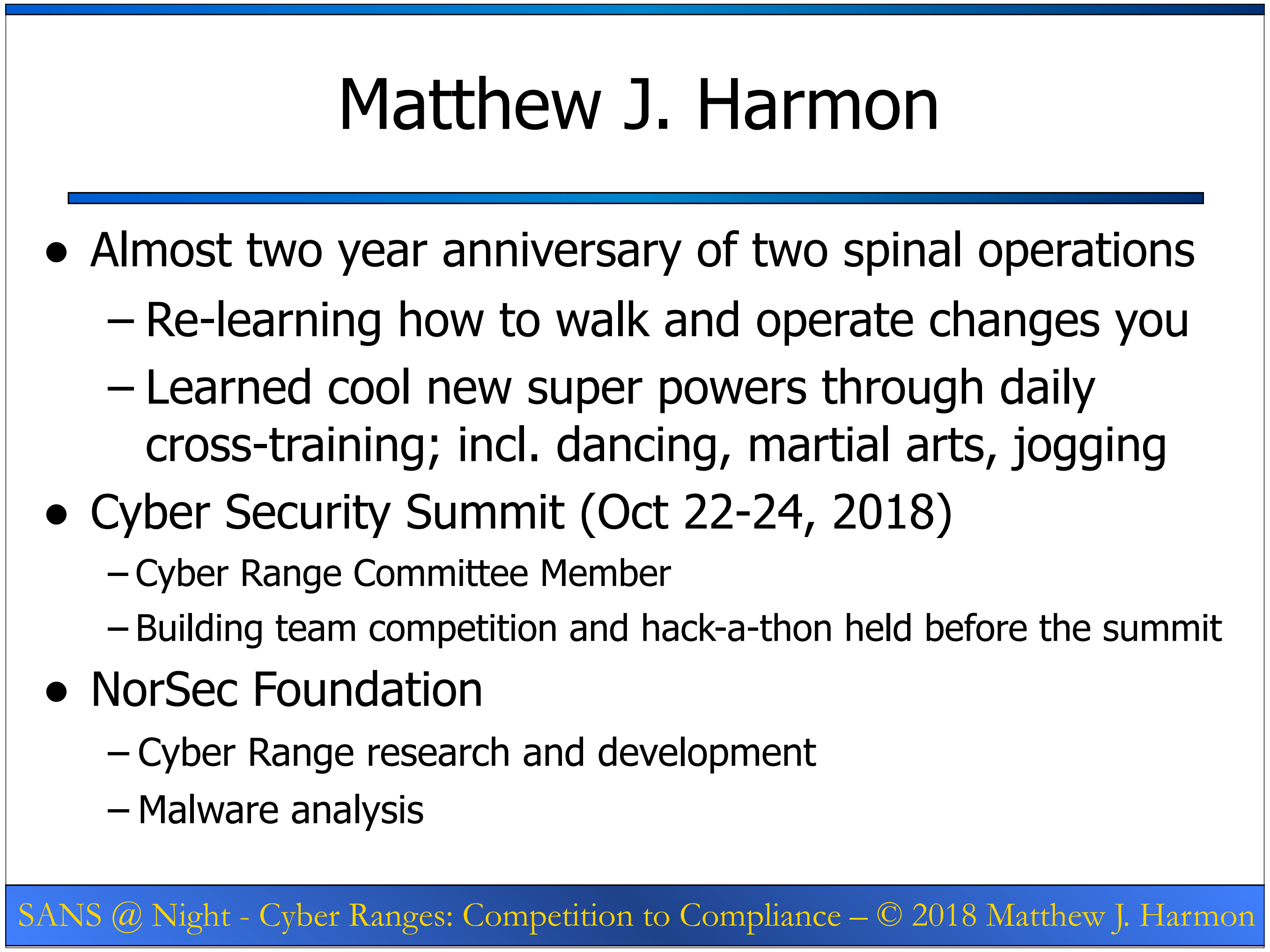
Hello everyone! Welcome to SANS @ Night, Emerging Cyber Ranges: From Competition to Compliance.



Matthew J. Harmon

- IT Risk Limited, Principal Consultant
  - GRC, Technology Risk Assessments, Remediation, Interim CISO
- SANS Community & Mentor, 10 year anniversary!
  - SEC 401 Security Essentials
  - SEC 504 Hacker Tools, Techniques, Exploits & Incident Handling
  - SEC 464 Hacker Guard, IT Operations Baselining
- St. Paul College, CompSci Course Author & Instructor:
  - 2461 70 & 71 Computer Networking 3 - Linux
  - 2480 40 Network Security & Penetration Prevention
  - 2482 40 Security Incident Handling, Response and Disaster Recovery
  - 2484 40 Ethical Hacking & Countermeasures

Hello everyone, my name is Matthew J Harmon I'm a Security Consultant, Network and Systems Engineer, a Course Author for Saint Paul College in the Computer Science department, and of course an Instructor for the SANS Institute. This is actually very close to the 10 year anniversary of my Murder Board with John Strand & Co. before teaching my first SEC 401 class, the Security Essentials Bootcamp. Fond memories of arguing the nuances of TCP/IP window sizes and when decreasing the window size, are the packets fragmented, or not?

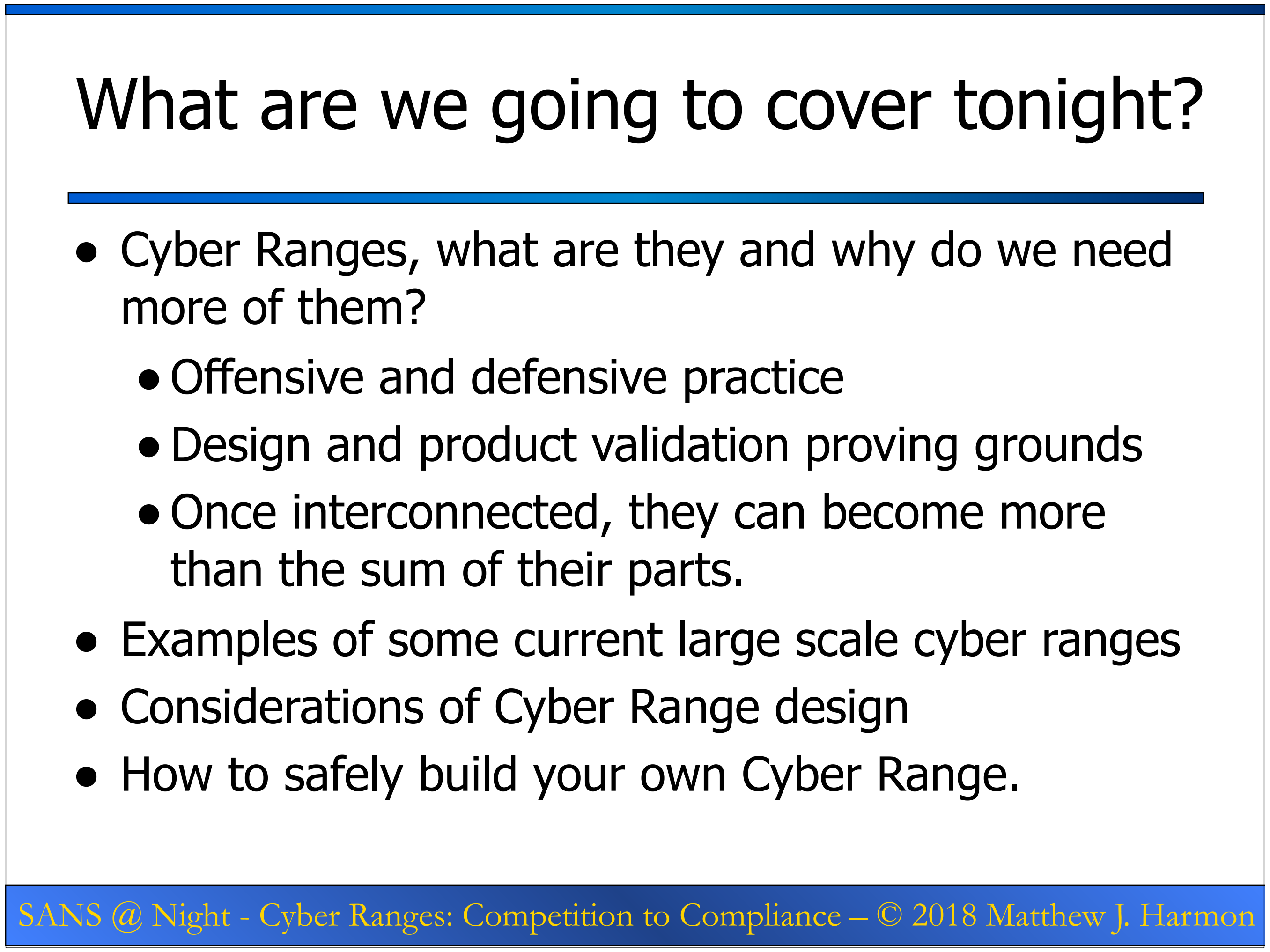


Matthew J. Harmon

- Almost two year anniversary of two spinal operations
  - Re-learning how to walk and operate changes you
  - Learned cool new super powers through daily cross-training; incl. dancing, martial arts, jogging
- Cyber Security Summit (Oct 22-24, 2018)
  - Cyber Range Committee Member
  - Building team competition and hack-a-thon held before the summit
- NorSec Foundation
  - Cyber Range research and development
  - Malware analysis

This month is also the two year anniversary of the emergency department admission that would later lead to two spinal operations to correct Cauda Equina Syndrome, a compression of the spinal nerve root, the result of an improperly healed injury then compounded by significant stress and a lifestyle that didn't allow for taking better care of myself. I've developed some cool super powers though, prior to the injury I never would practice martial arts, dance, jog, or for that matter do pull ups or push ups for fun.

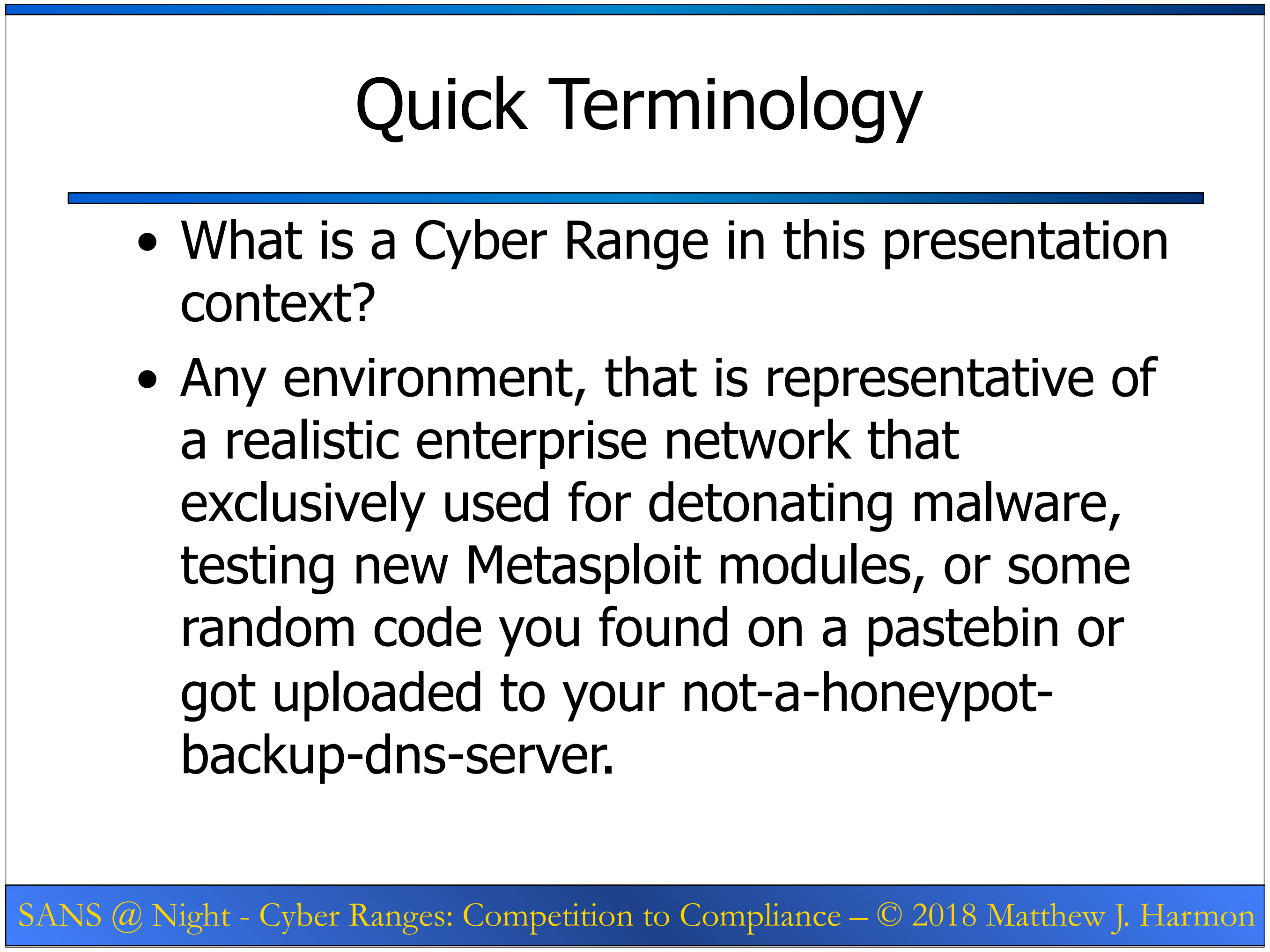
Getting back to tech wizardry and not super powers, I'm a member of the Cyber Security Summit Cyber Range Committee, we're working on bringing what we're going to be talking about tonight to a hack-a-thon and team competition at the event. This work has been made possible by the NorSec Foundation, supporting our research and development. Right now, we're looking for sponsors that want to contribute to building a network of Cyber Ranges for offensive and defensive security training and competition. **Yes, you heard that right, I really want to make Cyber eSports a thing.**



What are we going to cover tonight?

- Cyber Ranges, what are they and why do we need more of them?
  - Offensive and defensive practice
  - Design and product validation proving grounds
  - Once interconnected, they can become more than the sum of their parts.
- Examples of some current large scale cyber ranges
- Considerations of Cyber Range design
- How to safely build your own Cyber Range.

So, what are we going to cover tonight? We're going to talk about Cyber Ranges. What they are, why we need more of them, and how you can make them safely. Their usefulness for fun competition, education, a proving ground for strategies and tactics, but it is crucial that we start using them for compliance and to prove, or disprove, claims of security and technological safety.



Quick Terminology

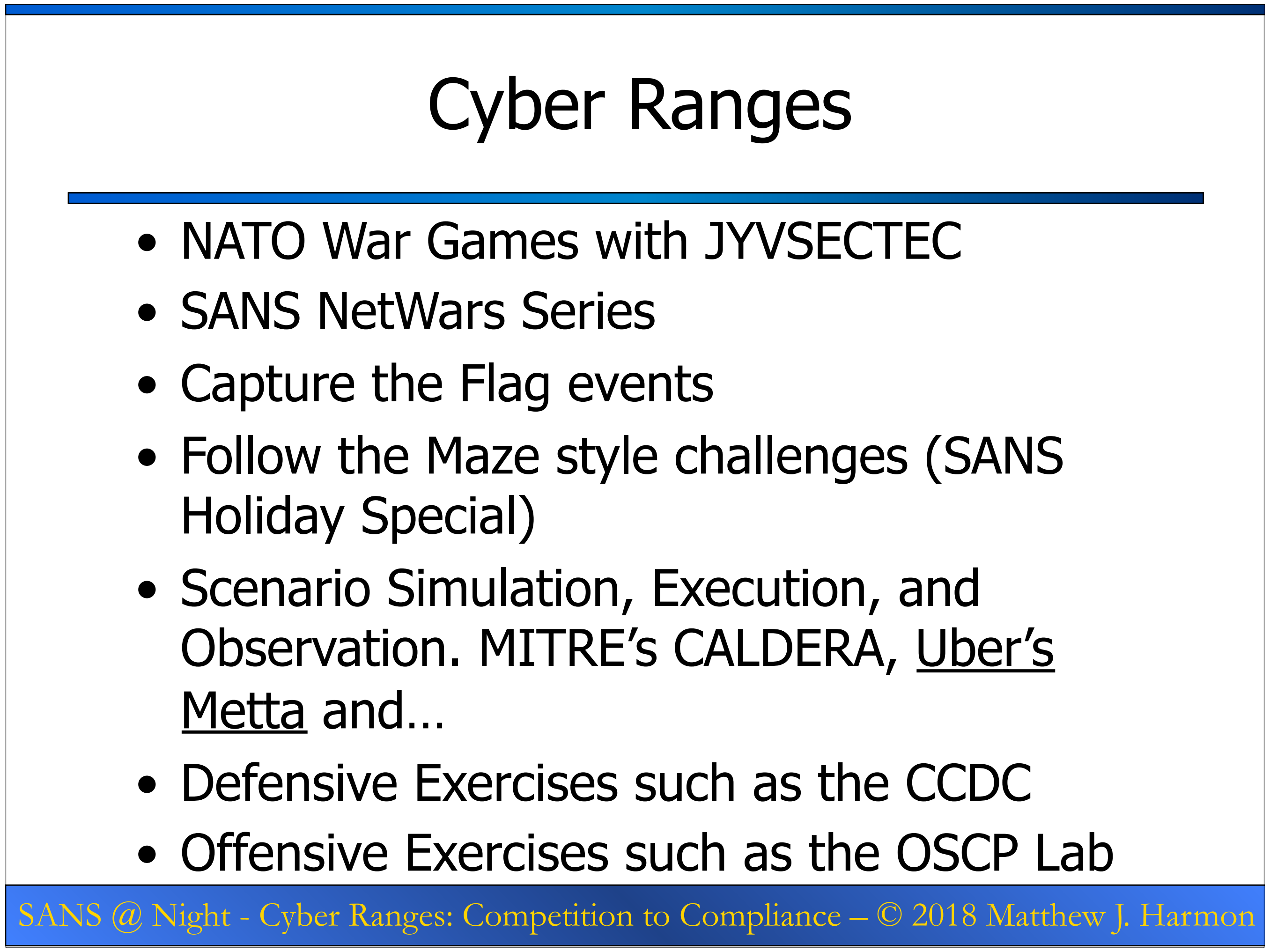
- What is a Cyber Range in this presentation context?
- Any environment, that is representative of a realistic enterprise network that exclusively used for detonating malware, testing new Metasploit modules, or some random code you found on a pastebin or got uploaded to your not-a-honeypot-backup-dns-server.

Let's start out with some quick terminology. In the context of this talk tonight, a Cyber Range is any contained environment that is disconnected from the Internet and your Internal Network, that is able to be quickly refreshed after detonating malware, testing a new exploit that you found on a PasteBin that was mentioned on Twitter, 4Chan, or TotallyNotaFed911.onion.

Is my dev environment a Cyber Range?

- No, but…
- We'll talk about shortly about how a Cyber Range can help your dev team.

Integrating a Cyber Range with your DevOps process brings red and blue teams together into a nice shade of purple. Training offensively allows developers to think offensively and build around application or framework weaknesses.



Cyber Ranges

- NATO War Games with JYVSECTEC
- SANS NetWars Series
- Capture the Flag events
- Follow the Maze style challenges (SANS Holiday Special)
- Scenario Simulation, Execution, and Observation. MITRE's CALDERA, Uber's Metta and…
- Defensive Exercises such as the CCDC
- Offensive Exercises such as the OSCP Lab

Other examples, include NATO's WarGames which JYVSECTEC supported, the SANS NetWars Series, Capture the Flag style events, Follow the Maze events like the SANS Holiday Special, Scenario Emulation, Execution and Observation systems like MITRE's CALDERA and Uber's Matte both of which use the MITRE ATT&CK enumeration system. Additionally, there are systems like the Cyber Collegiate Defense Competition that tests defensive skills, and of course the Offensive Security Certified Professional lab.

SANS NetWars: CyberCity

- 1:87 scale physical city.

https://www.sans.org/netwars/cybercity

SANS CyberCity is a 1:87 scale miniaturized physical city that features SCADA-controlled electrical power distribution, as well as water, transit, hospital, bank, retail, and residential infrastructures.

NetWars: DFIR Tournament

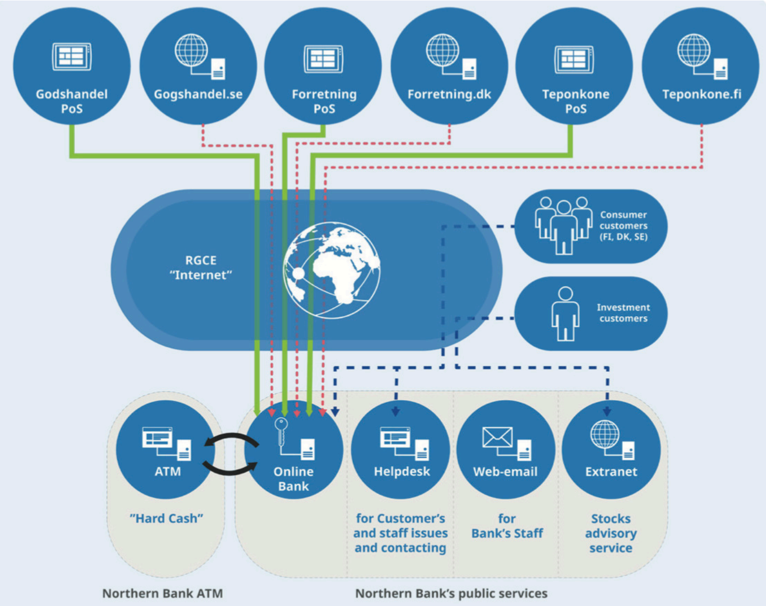
- Digital Forensics, Incident Response and Threat Hunting Scenarios

https://www.sans.org/netwars/dfir-tournament

SAND Digital Forensics and Incident Response Tournament

JYVSECTEC

- Financial organization, NorthernBank

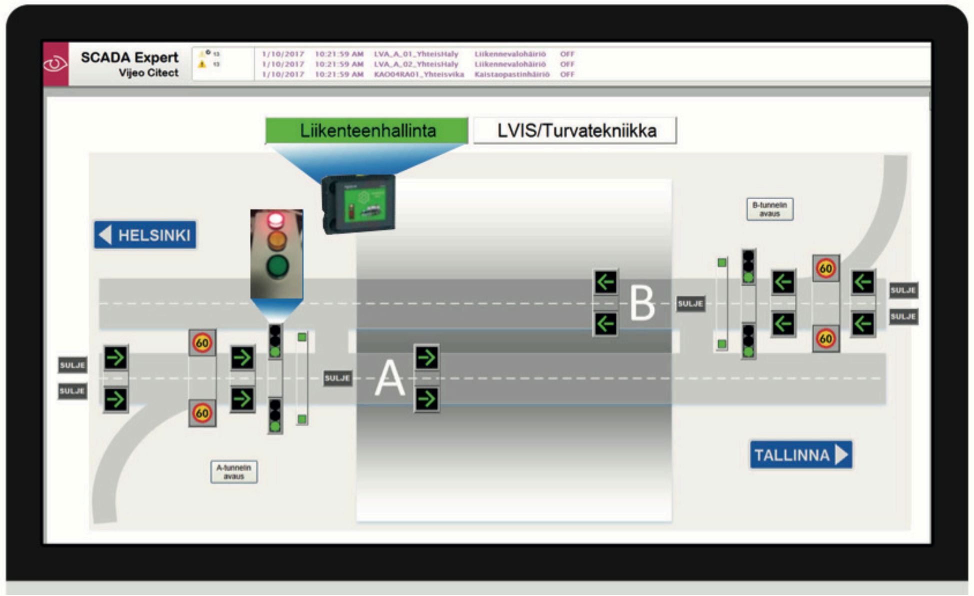


https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

JYVSECTEC out of Finland has made several full Cyber Ranges including a Financial Organization called NorthernBank. It includes simulation of payment processors, users, cash dispensary, and end-user payment systems.

JYVSECTEC

- Road tunnel provider, Funnel



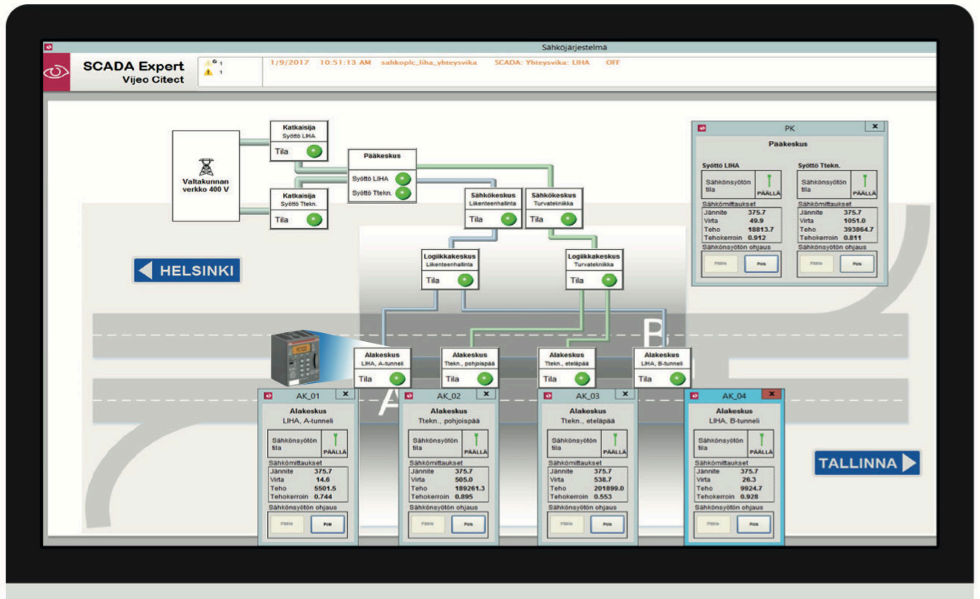
```
1/10/2017   10:21:59 AM   LVA_A_01_YhteisHaly     Liikennevalohäiriö     OFF
1/10/2017   10:21:59 AM   LVA_A_02_YhteisHaly     Liikennevalohäiriö     OFF
1/10/2017   10:21:59 AM   KAO04RA01_Yhteisvika    Kaistaopastinhäiriö    OFF
```

https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

JYVSECTEC also made Funnel, a Road tunnel provider. This terrific simulation includes all of the SCADA components for controlling traffic flow through a tunnel including.

JYVSECTEC

- Electricity Company, Watti



Sähköjärjestelmä

SCADA Expert Vijeo Citect

1/9/2017 10:51:13 AM sahkoplc_liha_yhteysvika SCADA: Yhteysvika: LIHA OFF

PK – Pääkeskus

Syöttö LIHA		Syöttö Ttekn.	
Sähkönsyötön tila	PÄÄLLÄ	Sähkönsyötön tila	PÄÄLLÄ
Sähkömittaukset		Sähkömittaukset	
Jännite	375.7	Jännite	375.7
Virta	49.9	Virta	1051.0
Teho	18813.7	Teho	393864.7
Tehokerroin	0.912	Tehokerroin	0.811

	AK_01	AK_02	AK_03	AK_04
Alakeskus	LIHA, A-tunneli	Ttekn., pohjoispää	Ttekn., eteläpää	LIHA, B-tunneli
Sähkönsyötön tila	PÄÄLLÄ	PÄÄLLÄ	PÄÄLLÄ	PÄÄLLÄ
Jännite	375.7	375.7	375.7	375.7
Virta	14.6	505.0	538.7	26.3
Teho	5501.5	189261.3	201899.0	9924.7
Tehokerroin	0.744	0.895	0.553	0.928

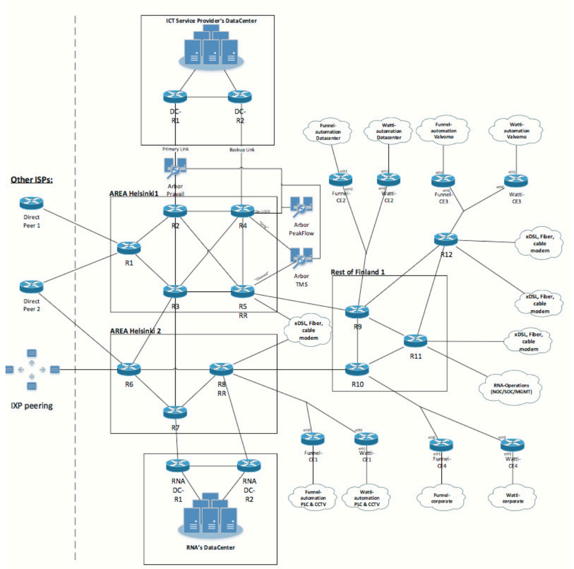
Valtakunnan verkko 400 V
Katkaisija Syöttö LIHA Tila
Katkaisija Syöttö Ttekn. Tila
Pääkeskus
Syöttö LIHA
Syöttö Ttekn.
Sähkökeskus Liikenteenhallinta Tila
Sähkökeskus Turvatekniikka Tila
Logiikkakeskus Liikenteenhallinta Tila
Logiikkakeskus Turvatekniikka Tila
Alakeskus LIHA, A-tunneli Tila
Alakeskus Ttekn., pohjoispää Tila
Alakeskus Ttekn., eteläpää Tila
Alakeskus LIHA, B-tunneli Tila
HELSINKI
TALLINNA
A
B
Sähkönsyötön ohjaus
Päälle
Pois

https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf

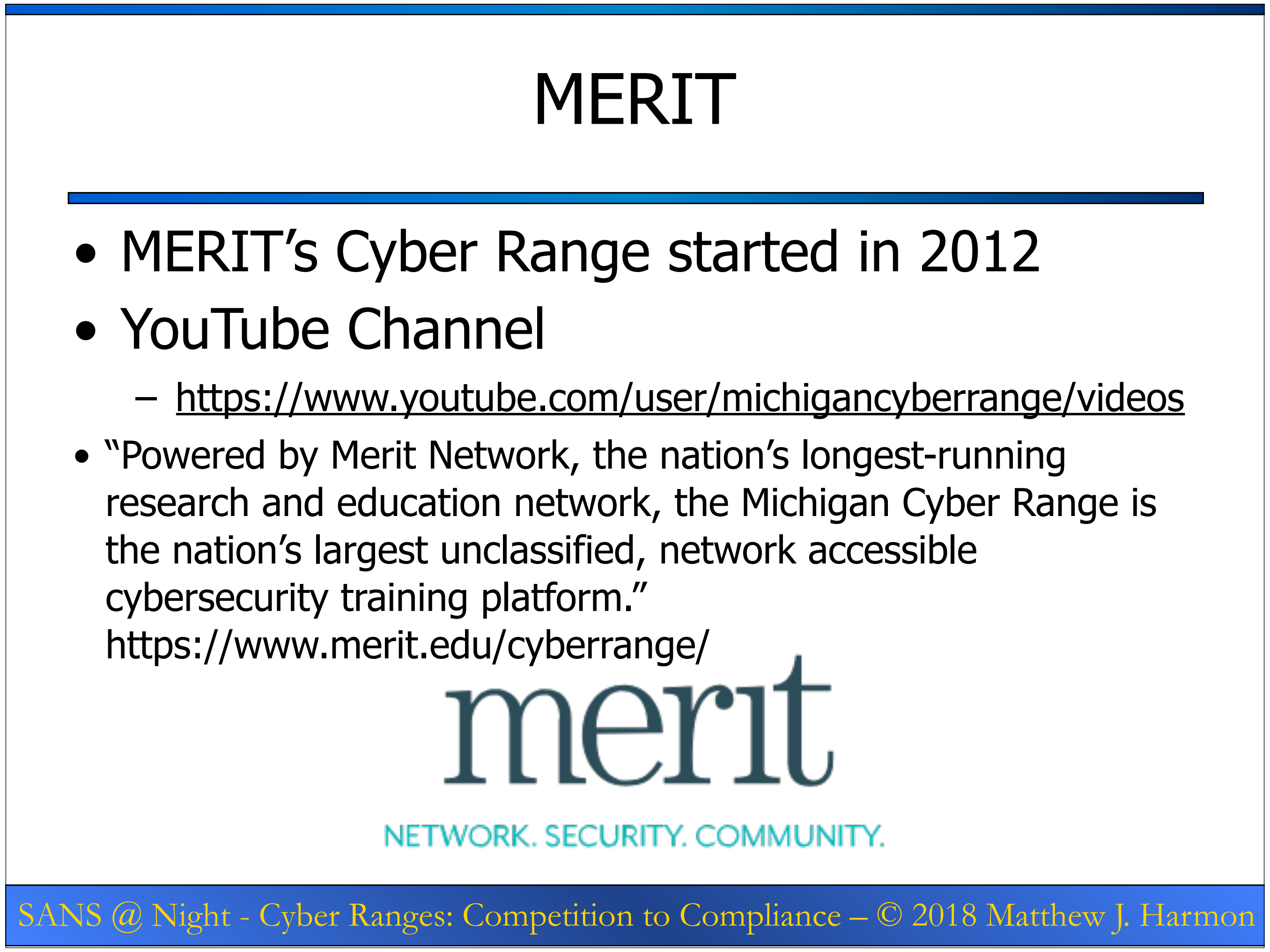
They also made Watti, an Electric Company, and an internet simulating Internet Service Provider RNA.

JYVSECTEC

- Internet Service Provider, RNA



https://jyvsectec.fi/wp-content/uploads/2017/02/JYVSECTEC-cyber-range.pdf



MERIT

- MERIT’s Cyber Range started in 2012
- YouTube Channel
  - https://www.youtube.com/user/michigancyberrange/videos
- “Powered by Merit Network, the nation’s longest-running research and education network, the Michigan Cyber Range is the nation’s largest unclassified, network accessible cybersecurity training platform.” https://www.merit.edu/cyberrange/

merit

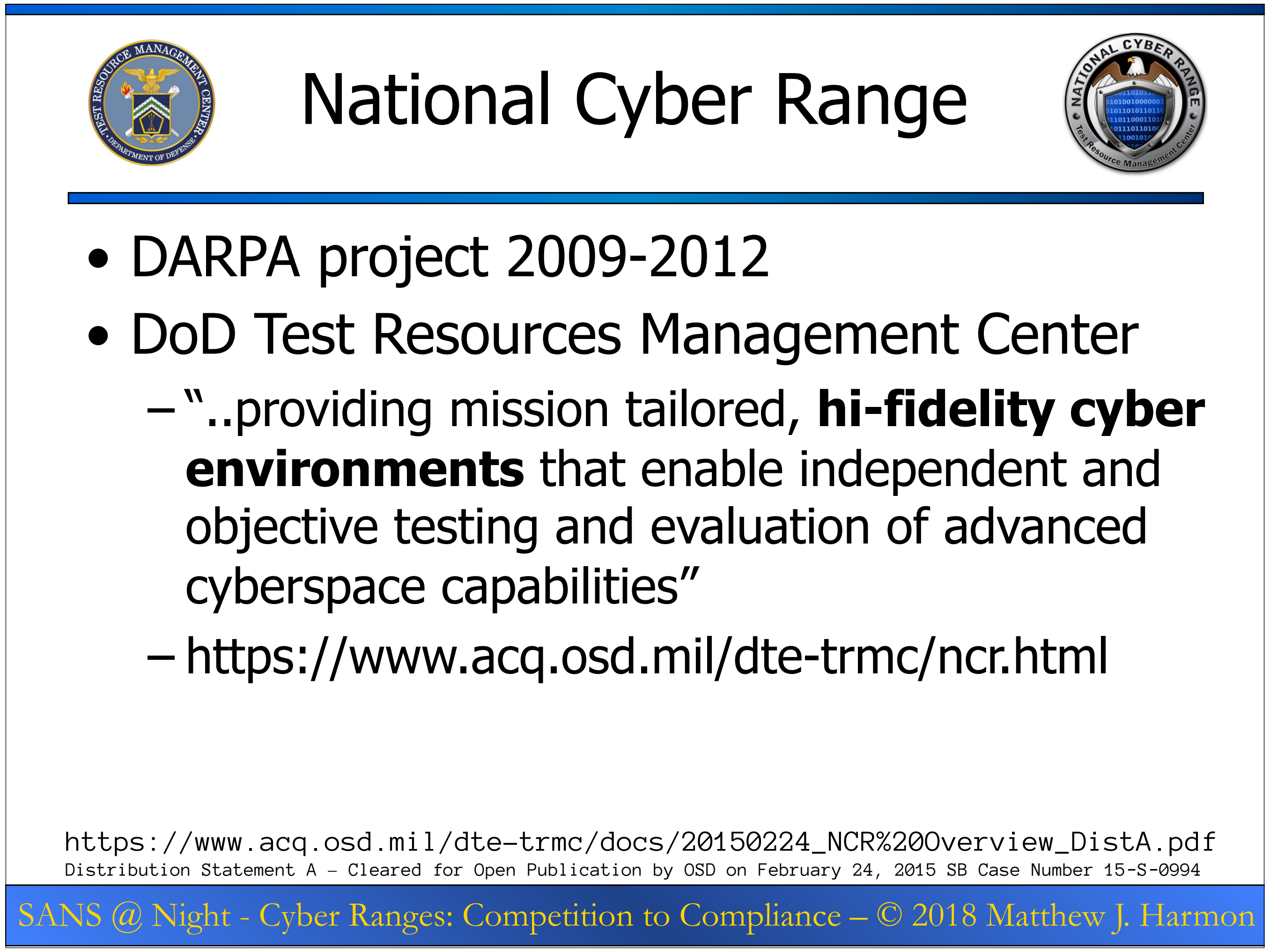
NETWORK. SECURITY. COMMUNITY.

Domestically, out of Michigan, MERIT's Cyber Range started in 2012 and is truly brilliant. They have a video page, but I think this following video shows what is possible when you get some gaming involved competing in Cyber Range eSports competitions takes on a new look.

MERIT's Alphaville

https://www.youtube.com/watch?v=9E08xSGviRI

Welcome to Alphaville.



National Cyber Range

- DARPA project 2009-2012
- DoD Test Resources Management Center
  - "..providing mission tailored, **hi-fidelity cyber environments** that enable independent and objective testing and evaluation of advanced cyberspace capabilities"
  - https://www.acq.osd.mil/dte-trmc/ncr.html

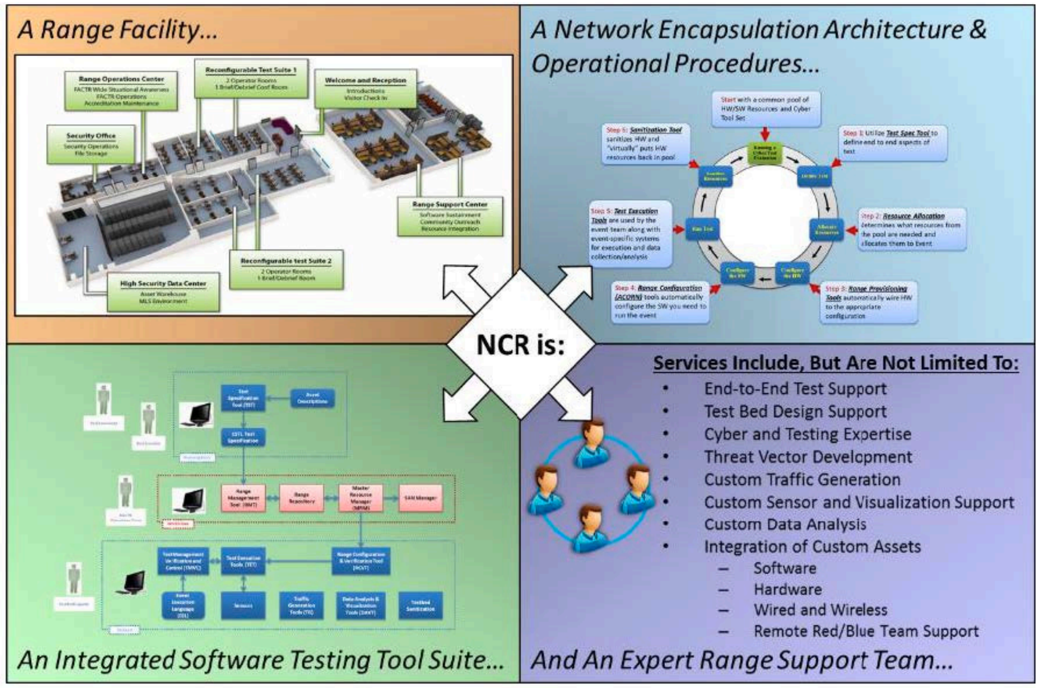
https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

Looking at this from a military perspective, the United States Defense Advanced Research Projects Agency, DARPA, started a National Cyber Range in 2009 and managed it until 2012 when the Test Resources Management Center took on the mission of providing mission tailored, hi-fidelity cyber environments for testing and evaluation.

The National Cyber Range consists of multiple facilities that provide a full service testing environment. The key components for creating ones own cyber range include the reconfigurable test suite and high security data center.

National Cyber Range

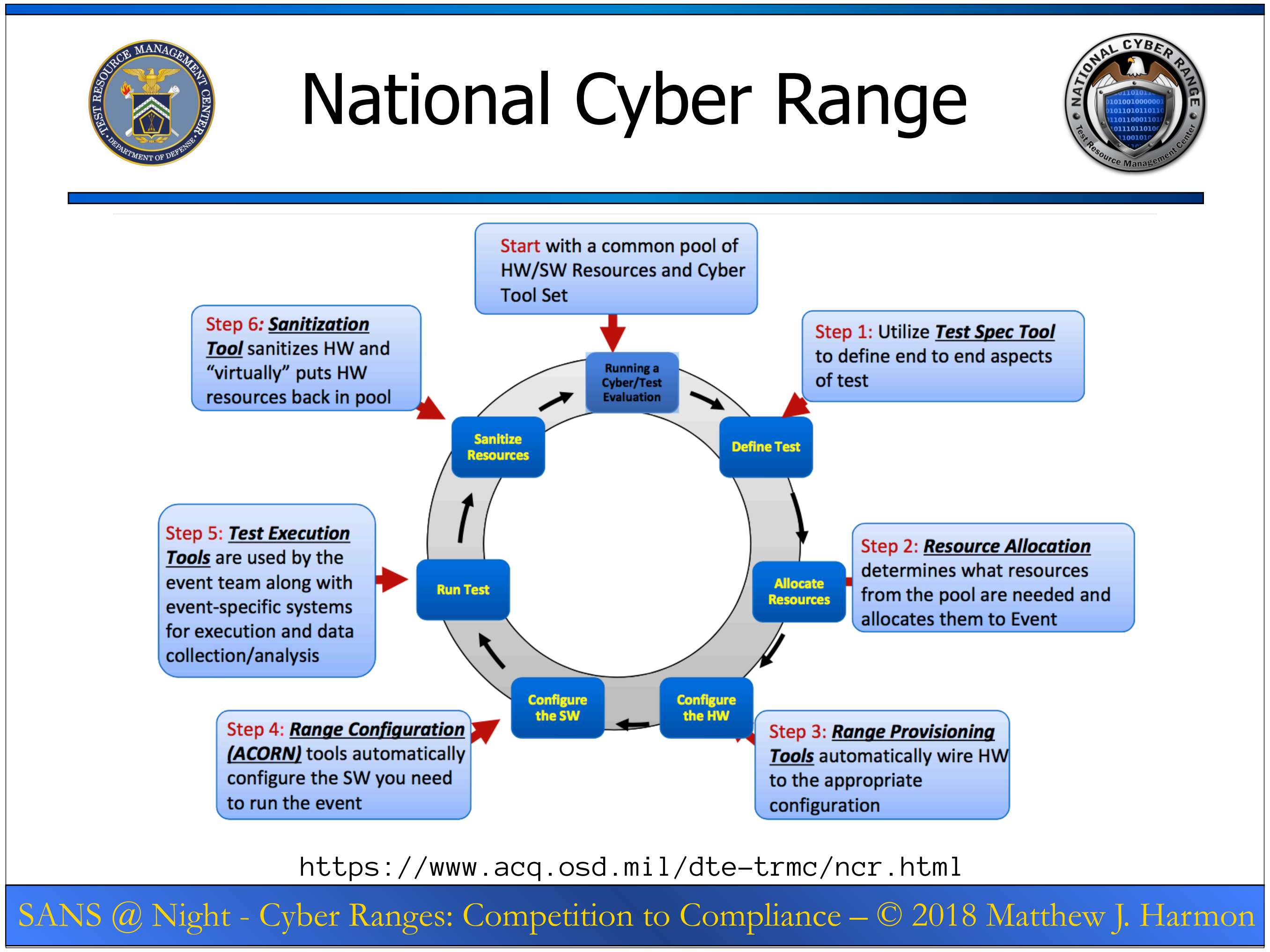

A Range Facility...
Range Operations Center
FACTR Wide Situational Awareness
FACTR Operations
Accreditation Maintenance
Reconfigurable Test Suite 1
2 Operator Rooms
1 Brief/Debrief Conf Room
Welcome and Reception
Introductions
Visitor Check In
Security Office
Security Operations
File Storage
Range Support Center
Software Sustainment
Community Outreach
Resource Integration
Reconfigurable test Suite 2
2 Operator Rooms
1 Brief/Debrief Room
High Security Data Center
Asset Warehouse
MLS Environment
A Network Encapsulation Architecture & Operational Procedures...
Start with a common pool of HW/SW Resources and Cyber Tool Set
Step 1: Utilize Test Spec Tool to define end to end aspects of test
Step 2: Resource Allocation determines what resources from the pool are needed and allocates them to Event
Step 3: Range Provisioning Tools automatically wire HW to the appropriate configuration
Step 4: Range Configuration (ACORN) tools automatically configure the SW you need to run the event
Step 5: Test Execution Tools are used by the event team along with event-specific systems for execution and data collection/analysis
Step 6: Sanitization Tool sanitizes HW and "virtually" puts HW resources back in pool
Allocate Resources
Configure the HW
Configure the SW
Run Test
NCR is:
An Integrated Software Testing Tool Suite...
And An Expert Range Support Team...

Services Include, But Are Not Limited To:

- End-to-End Test Support
- Test Bed Design Support
- Cyber and Testing Expertise
- Threat Vector Development
- Custom Traffic Generation
- Custom Sensor and Visualization Support
- Custom Data Analysis
- Integration of Custom Assets
  - Software
  - Hardware
  - Wired and Wireless
  - Remote Red/Blue Team Support

https://www.acq.osd.mil/dte-trmc/ncr.html

In the upper left is the range facility, which we'll get to next. In the bottom right, in **purple**, is the support team building and maintaining the Cyber Range. In the bottom left, in **green**, is the software test suite including the components that provide mission support.



National Cyber Range

Start with a common pool of HW/SW Resources and Cyber Tool Set

Step 1: Utilize ***Test Spec Tool*** to define end to end aspects of test

Step 2: ***Resource Allocation*** determines what resources from the pool are needed and allocates them to Event

Step 3: ***Range Provisioning Tools*** automatically wire HW to the appropriate configuration

Step 4: ***Range Configuration (ACORN)*** tools automatically configure the SW you need to run the event

Step 5: ***Test Execution Tools*** are used by the event team along with event-specific systems for execution and data collection/analysis

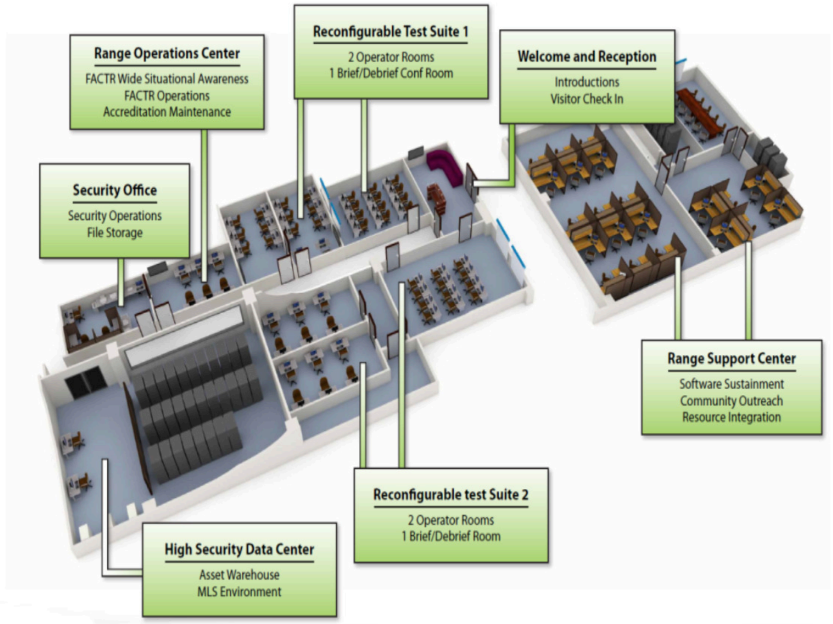
Step 6: ***Sanitization Tool*** sanitizes HW and "virtually" puts HW resources back in pool

https://www.acq.osd.mil/dte-trmc/ncr.html

SANS @ Night - Cyber Ranges: Competition to Compliance – © 2018 Matthew J. Harmon

The Operational Procedures include hardware and software definition at the 12 O'Clock position, the expected results at 2 O'Clock then continuing clockwise we work through resource allocation, tool provisioning and configuration, range configuration loaded into the tool being tested, and then the actual test execution at 9 O'Clock including event specific simulations, finalizing with sanitizing of the environment and device being tested.

National Cyber Range

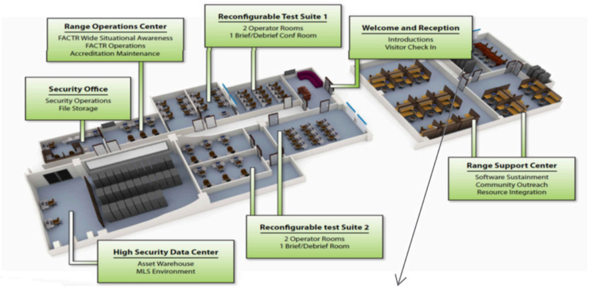


https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

To use a Scepter of Goth, or Dungeons & Dragons analogy
Here we get a closer look at the Range Operations Center (these are the Dungeon Masters), and in the Reconfigurable Test suites are two competing clans, the Range Support Center are the Non-Player Characters that clean up after you and without their help you'd never complete your missing, the NPC's that keep everything working - or not depending on your mission training. Your character sheets are stored with the Security Office, and your world lives in the high security data center.

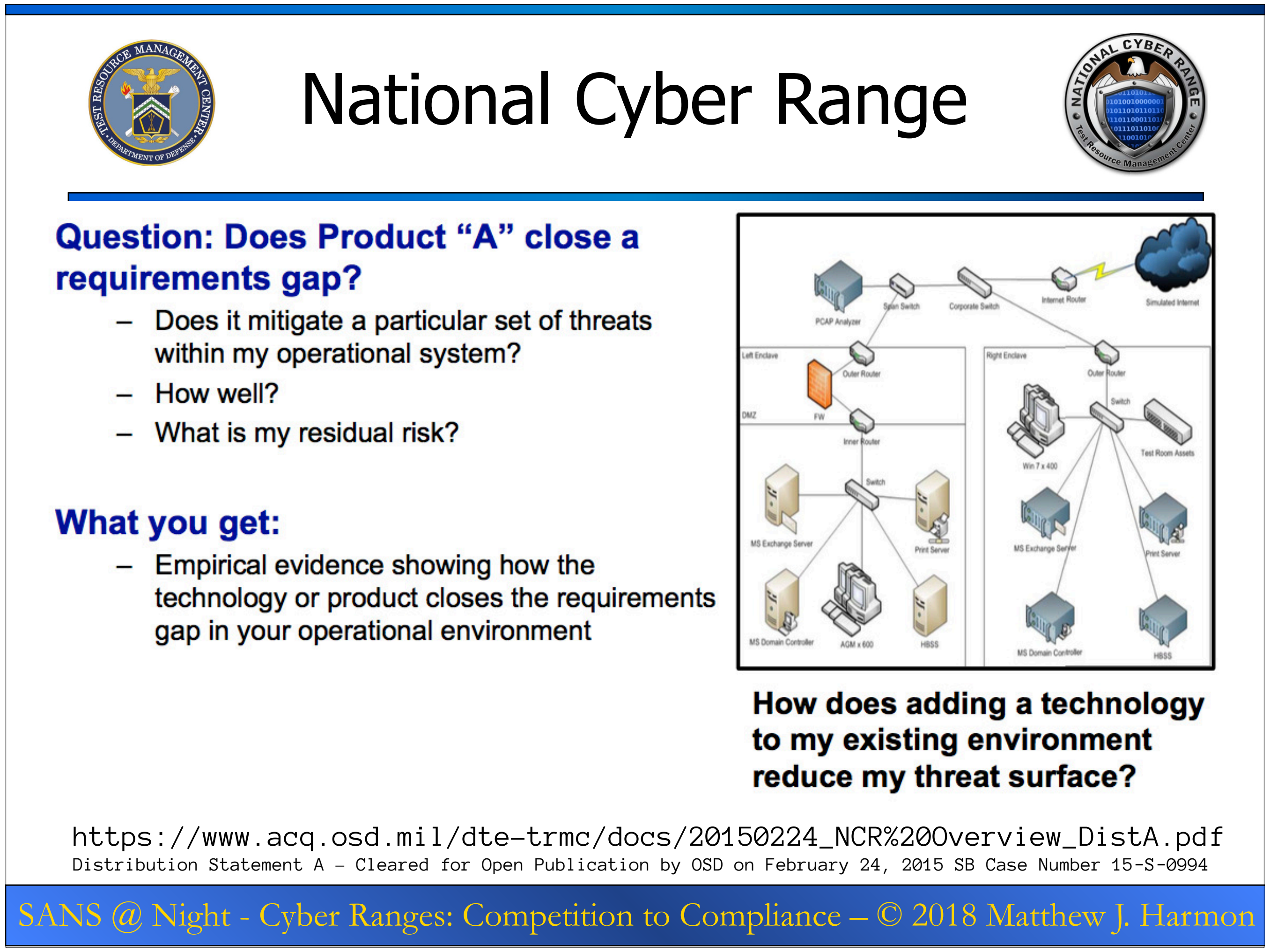
National Cyber Range



https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

For those of us who don't have the resources of DARPA available, there is still a significant amount we can learn from this work and specifically apply to our collective benefit, and that is asking "Does Product "A" close a requirements gap?". That is "How does adding a technology to my existing environment reduce my threat surface?" For many of us that are evaluating security products and fielding sales calls, this is where we can get extra credit for pitching your own Cyber Range to work as a liaison third party risk, contract/legal, and when not in use a playground for Doing Evil(tm).



National Cyber Range

Question: Does Product "A" close a requirements gap?

- Does it mitigate a particular set of threats within my operational system?
- How well?
- What is my residual risk?

What you get:

- Empirical evidence showing how the technology or product closes the requirements gap in your operational environment

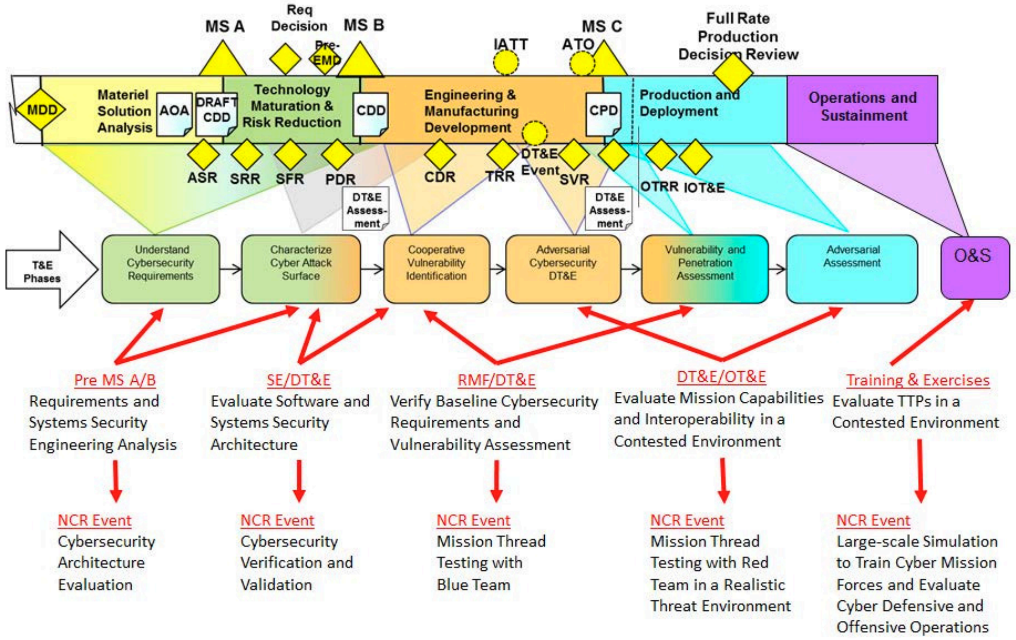
How does adding a technology to my existing environment reduce my threat surface?

https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf

Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

- In this scenario, we have a left and right enclave, a spanning switch, a corporate switch an internet router and the simulated internet.
- Preferably, this environment simulates the full internet, but at a minimum you need to have all of your enterprise services and a daily-snapshot of your development environment. This environment uses the SneakerNet to get data in, and results are SneakerNet walked out through a clean system.
- In the left enclave, you have the simulated environment for a Microsoft enterprise including Domain Controller, Exchange Server, Print Server, and 600 users with a firewall before the outer router.
- In the right enclave emulating a remote facility, you have 400 Windows 7 users, and the rest of the Microsoft enterprise.

Integrating Compliance


MS A
Req Decision
MS B
Pre-EMD
IATT
MS C
ATO
Full Rate Production Decision Review
MDD
Materiel Solution Analysis
AOA
DRAFT CDD
Technology Maturation & Risk Reduction
CDD
Engineering & Manufacturing Development
CPD
Production and Deployment
Operations and Sustainment
ASR
SRR
SFR
PDR
CDR
TRR
DT&E Event
SVR
OTRR
IOT&E
DT&E Assess-ment
DT&E Assess-ment
T&E Phases
Understand Cybersecurity Requirements
Characterize Cyber Attack Surface
Cooperative Vulnerability Identification
Adversarial Cybersecurity DT&E
Vulnerability and Penetration Assessment
Adversarial Assessment
O&S

Pre MS A/B
Requirements and Systems Security Engineering Analysis

NCR Event
Cybersecurity Architecture Evaluation

SE/DT&E
Evaluate Software and Systems Security Architecture

NCR Event
Cybersecurity Verification and Validation

RMF/DT&E
Verify Baseline Cybersecurity Requirements and Vulnerability Assessment

NCR Event
Mission Thread Testing with Blue Team

DT&E/OT&E
Evaluate Mission Capabilities and Interoperability in a Contested Environment

NCR Event
Mission Thread Testing with Red Team in a Realistic Threat Environment

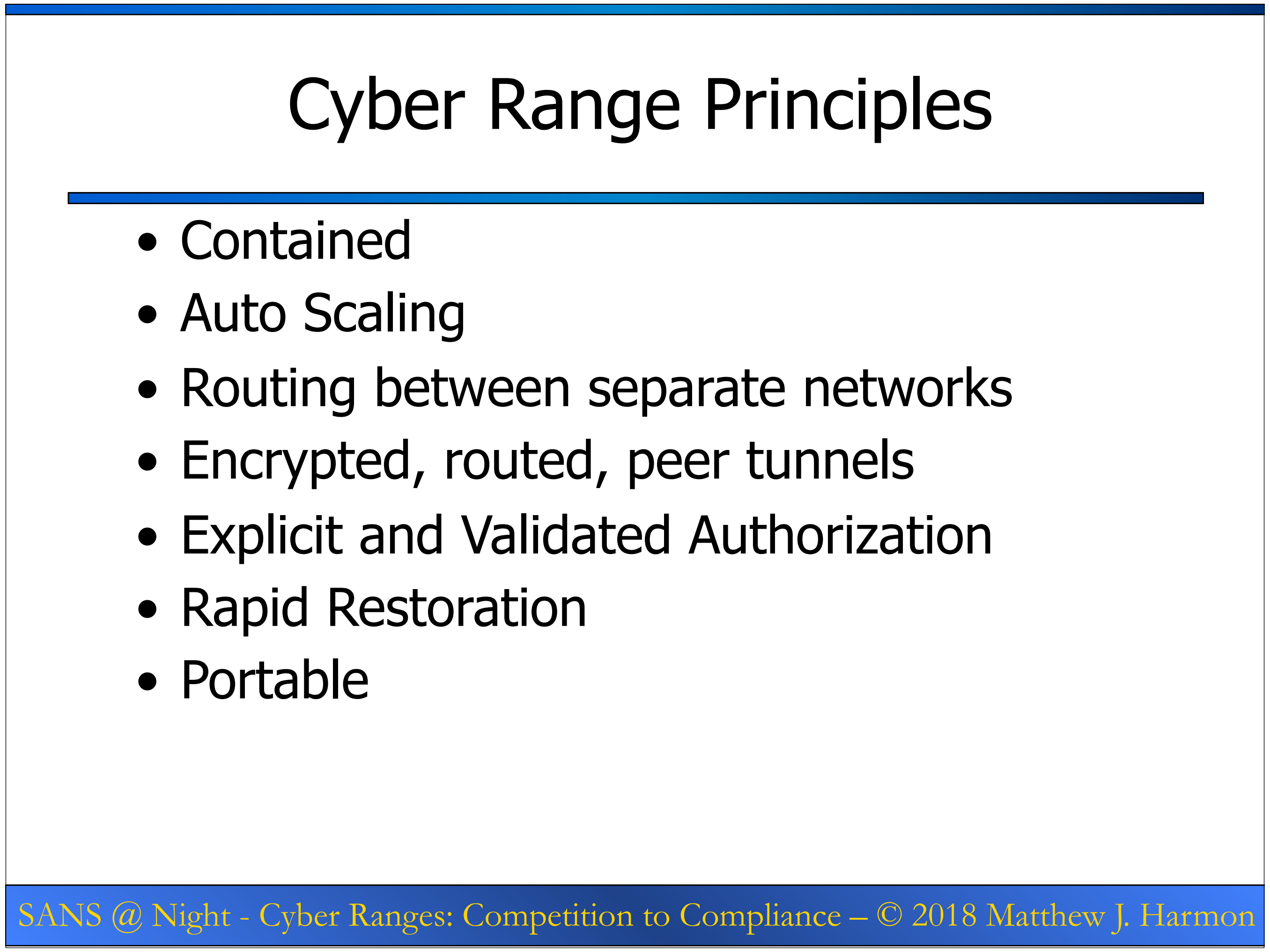
Training & Exercises
Evaluate TTPs in a Contested Environment

NCR Event
Large-scale Simulation to Train Cyber Mission Forces and Evaluate Cyber Defensive and Offensive Operations

https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf
Distribution Statement A – Cleared for Open Publication by OSD on February 24, 2015 SB Case Number 15-S-0994

This is where we can integrate the Cyber Range components into compliance. Each step of the acquisition, development, engineering, or testing process fits into a Cyber Range. Directly, when setting requirements at the beginning, through the evaluation of vendors and systems security architecture, then baselining and verifying the baseline and conducting vulnerability assessments, then aggressive testing for resiliency and decreased threat footprint, and finally within large scale simulations of your environment as the process becomes normalized.

Taking a short brain break, here we have A Starry Minneapolis Night. Author unknown. I found it and saved it from reddit slash r minneapolis some years ago. TinEye has some similar results, but nothing quite like this one.



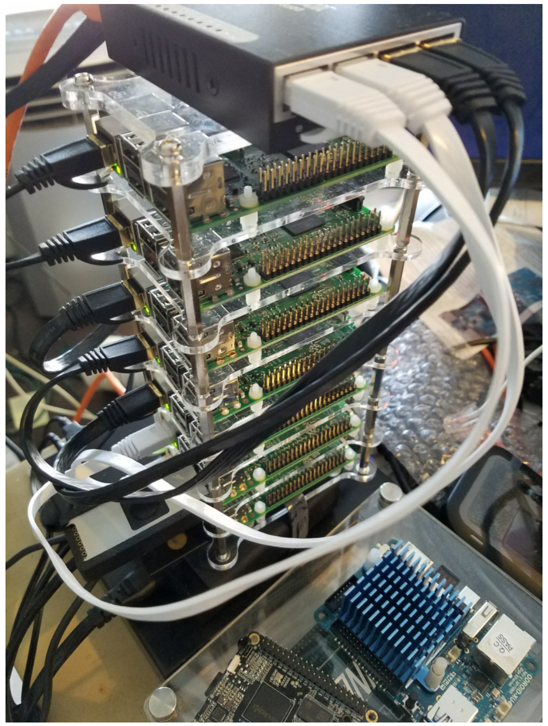
Cyber Range Principles

- Contained
- Auto Scaling
- Routing between separate networks
- Encrypted, routed, peer tunnels
- Explicit and Validated Authorization
- Rapid Restoration
- Portable

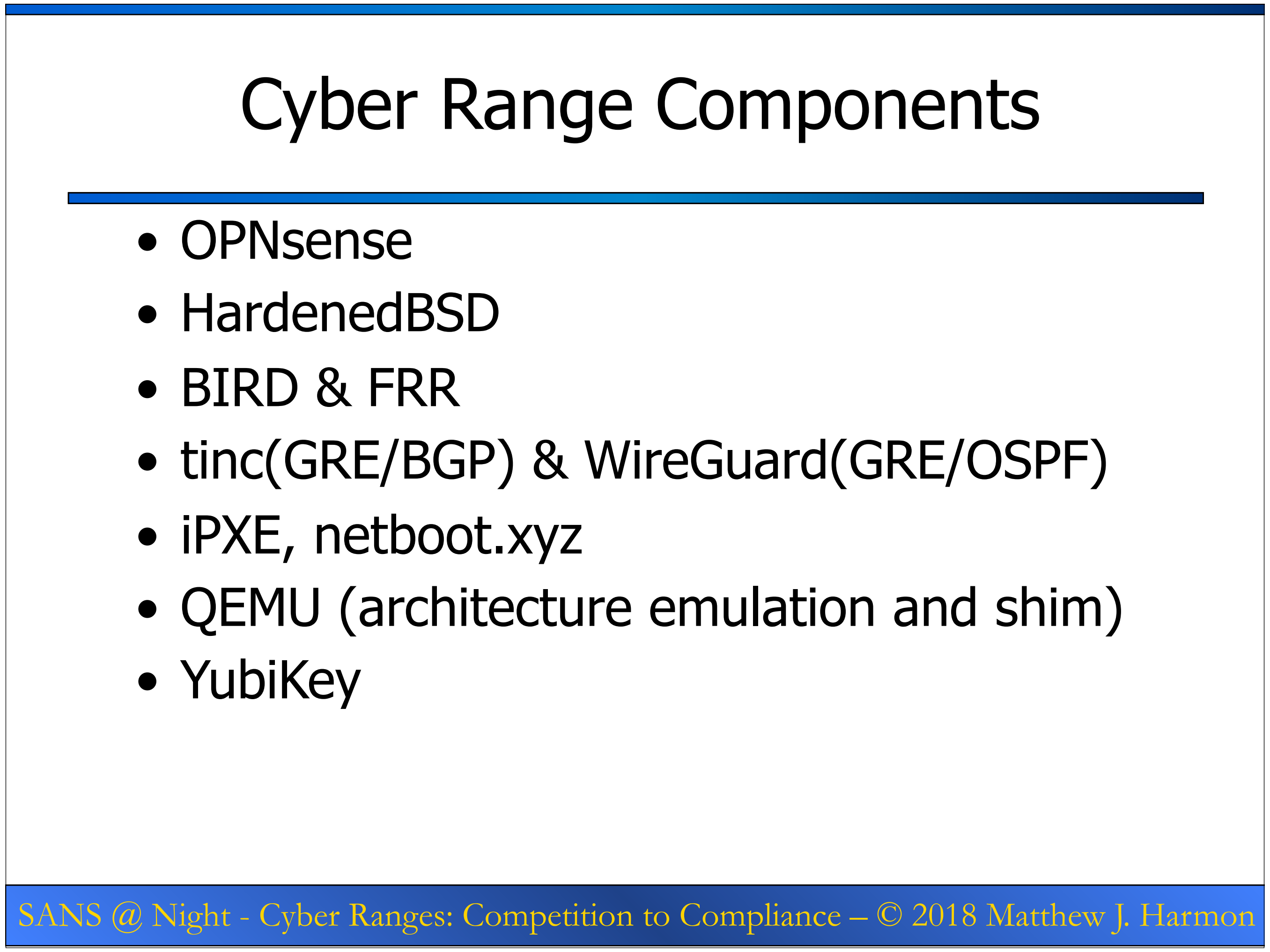
Like most of us, you don't have the budget of the Department of Defense but you still want to make a cyber range. You're going to want to keep it contained, auto scaling as you add resources, be able to route between other private ranges run by your friends, use encrypted routed peer tunnels at all times, make sure all authorized is explicit and validated, rapidly restorable, and for competitions you want this to be portable.

Proof of Concept

- Raspberry Pi Cluster
- apu2c4
- OPNsense
- USB Armory
- YubiKey
- Modeled after dn42



Here is our first Proof of Concept, seven Raspberry Pi's connected through a Blackbox powered hub, and sitting on-top of a PC Engines APU2C4. This utilizes a USB Armory running a custom Debian Linux installation as a Hardware Security Module with the YubiKey handling the key storage.



Cyber Range Components

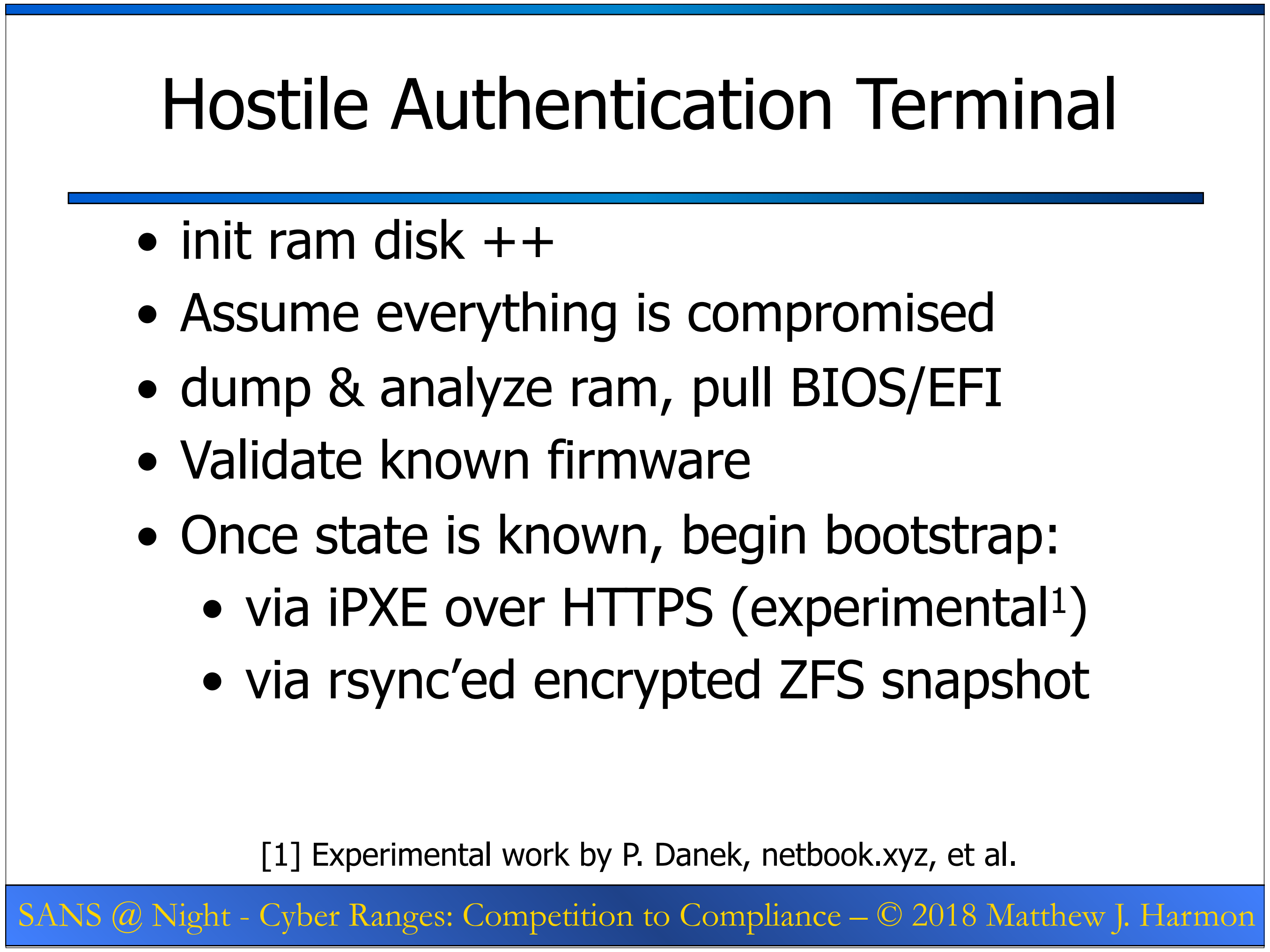
- OPNsense
- HardenedBSD
- BIRD & FRR
- tinc(GRE/BGP) & WireGuard(GRE/OSPF)
- iPXE, netboot.xyz
- QEMU (architecture emulation and shim)
- YubiKey

In this setup, one RaspberryPi is dedicated for serving images over iPXE and key management via the certificate authority running on the USB Armory. The another is the management route-server running BIRD and WireGuard. The APU2C4 is running OPNsense which is built on top of HardenedBSD, which is running tinc. OPNsense was chosen over pfSense as OPNsense using HardenedBSD and proactively integrates security features. The other five devices are available for attack and defense scenarios.

CrowdSupply Circumference

https://www.crowdsupply.com/ground-electronics/circumference/

The next time we setup this portable model, we'll most likely be using Ground Electronics Circumference currently available on CrowdSupply.

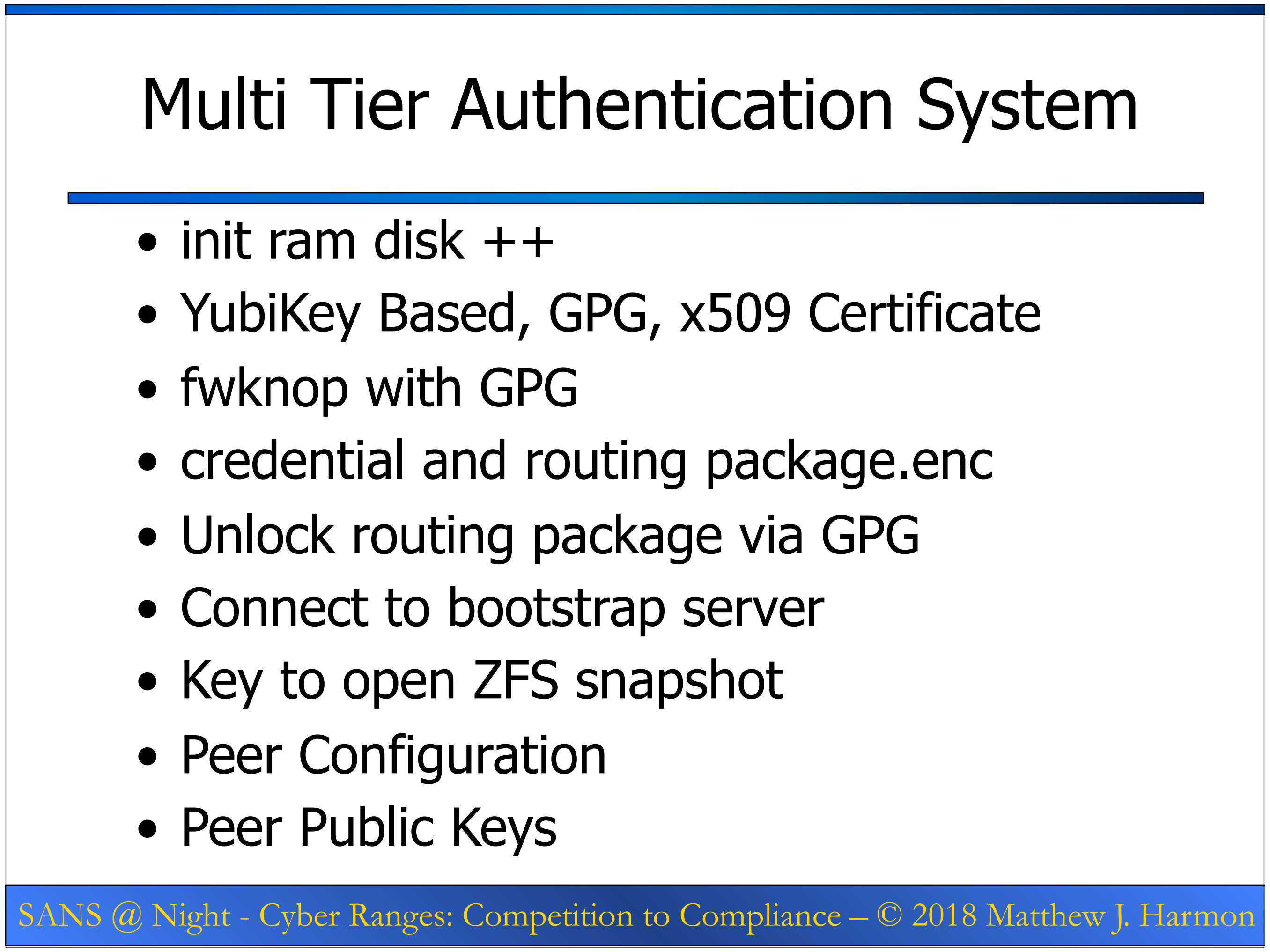


Hostile Authentication Terminal

- init ram disk ++
- Assume everything is compromised
- dump & analyze ram, pull BIOS/EFI
- Validate known firmware
- Once state is known, begin bootstrap:
  - via iPXE over HTTPS (experimental[1])
  - via rsync'ed encrypted ZFS snapshot

[1] Experimental work by P. Danek, netbook.xyz, et al.

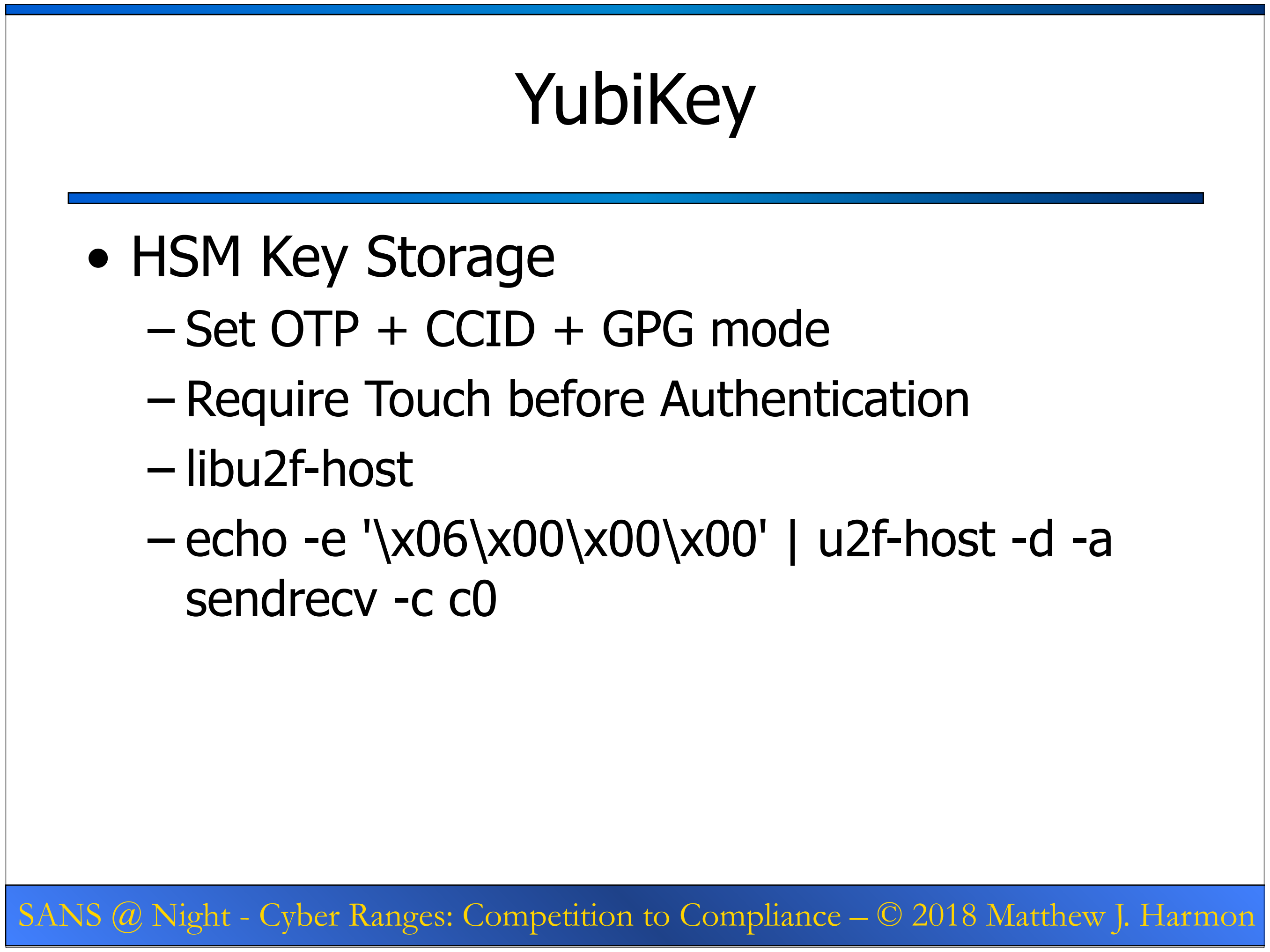
In order to securely deploy this, we created two nifty tools we'll be releasing once we clean them up a bit. The first is the H.A.T., the Hostile Authentication Terminal, which is used to verify the system and bootstrap prior to loading data.



Multi Tier Authentication System

- init ram disk ++
- YubiKey Based, GPG, x509 Certificate
- fwknop with GPG
- credential and routing package.enc
- Unlock routing package via GPG
- Connect to bootstrap server
- Key to open ZFS snapshot
- Peer Configuration
- Peer Public Keys

The second is M.T.A.S. or M-Taz which handles authentication and credential packages enabling the route server.

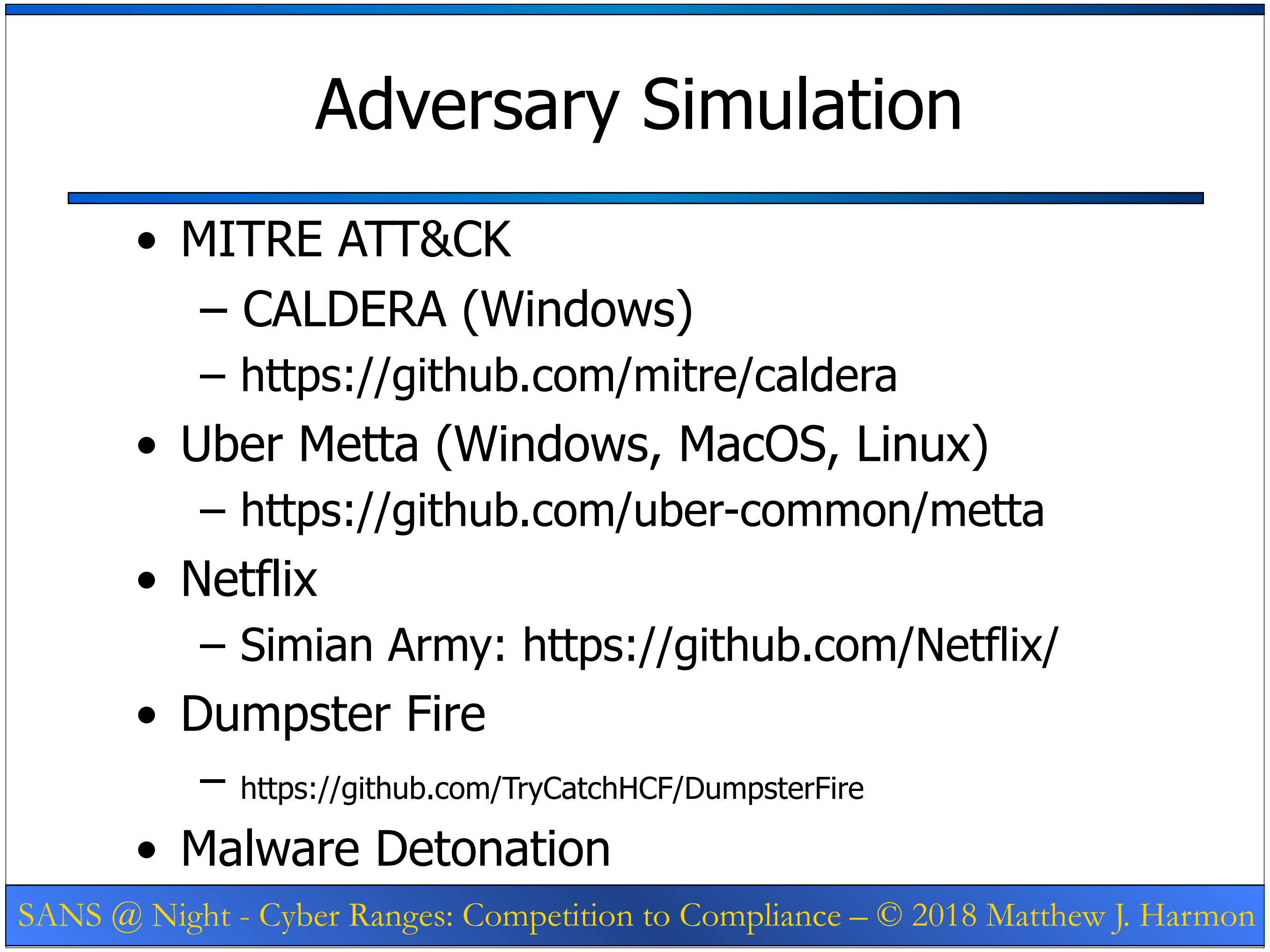


YubiKey

- HSM Key Storage
  - Set OTP + CCID + GPG mode
  - Require Touch before Authentication
  - libu2f-host
  - echo -e '\x06\x00\x00\x00' | u2f-host -d -a sendrecv -c c0

```
echo -e '\x06\x00\x00\x00' | u2f-host -d -a sendrecv -c c0
```

The YubiKey has made a lot of this possible operating as a Hardware Security Module, the ability to use x509 certificates as well as storing derivative GPG keys enables strong authentication in one multi-function device.



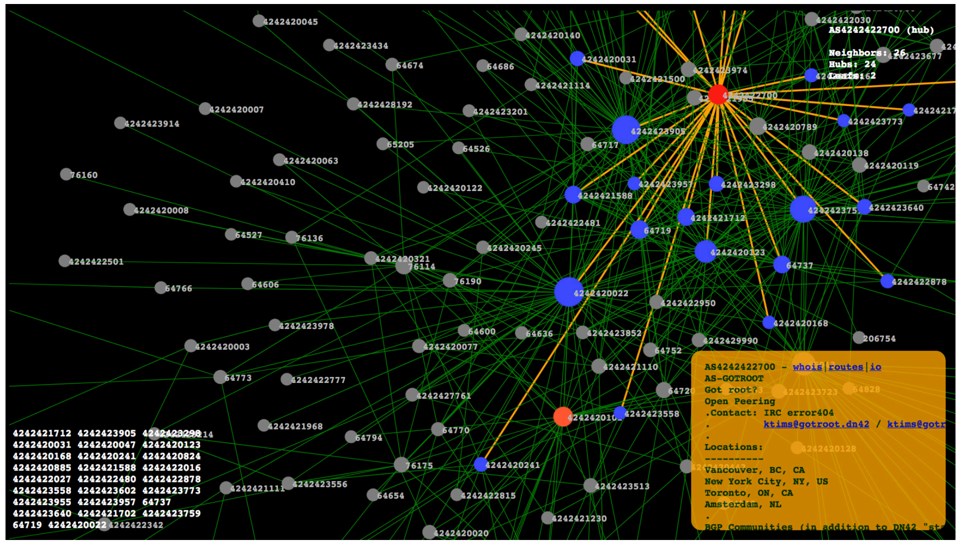
Adversary Simulation

- MITRE ATT&CK
  - CALDERA (Windows)
  - https://github.com/mitre/caldera
- Uber Metta (Windows, MacOS, Linux)
  - https://github.com/uber-common/metta
- Netflix
  - Simian Army: https://github.com/Netflix/
- Dumpster Fire
  - https://github.com/TryCatchHCF/DumpsterFire
- Malware Detonation

Simian Army - Chaos Monkey (which you’ve probably heard about) it randomly takes down systems. Janitor Monkey cleans up temp files and other remnants. Conformity Monkey checks for configurations, settings and ensure that the system is as expected.

dn42

- Security Research Network



```
AS4242422700 (hub)

Neighbors: 26
Hubs: 24
Leafs: 2
```

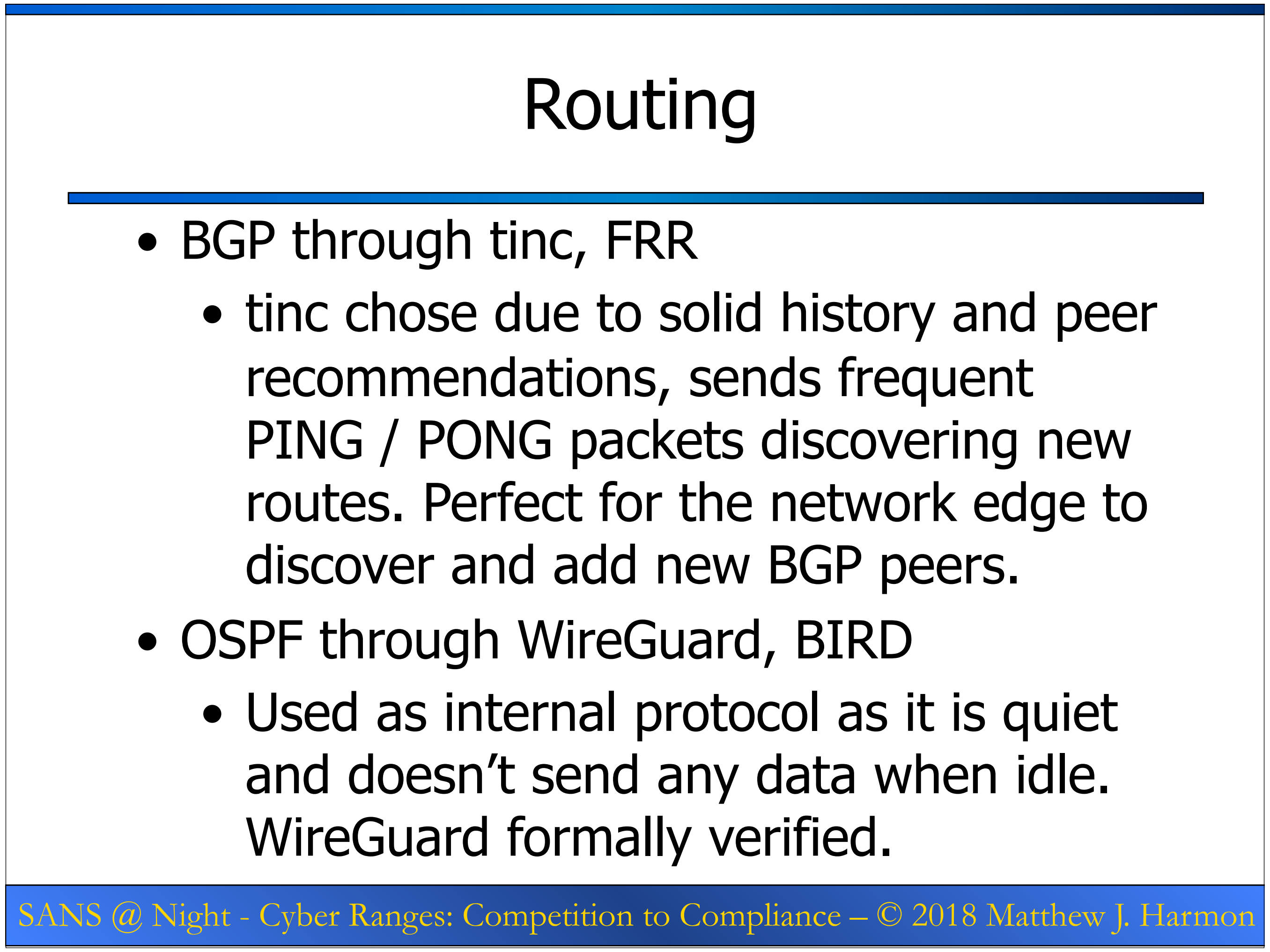
```
AS4242422700 - whois|routes|io
AS-GOTROOT
Got root?
Open Peering
.Contact: IRC error404
.          ktims@gotroot.dn42 / ktims@gotr
.
Locations:
----------
Vancouver, BC, CA
New York City, NY, US
Toronto, ON, CA
Amsterdam, NL
.
BGP Communities (in addition to DN42 "sta
```

```
4242421712 4242423905 4242423298
4242420031 4242420047 4242420123
4242420168 4242420241 4242420824
4242420885 4242421588 4242422016
4242422027 4242422480 4242422878
4242423558 4242423602 4242423773
4242423955 4242423957 64737
4242423640 4242421702 4242423759
64719 4242420022
```

https://nixnodes.net/dn42/graph/

NOTE: I have no relation to dn42, only great admiration for their work.

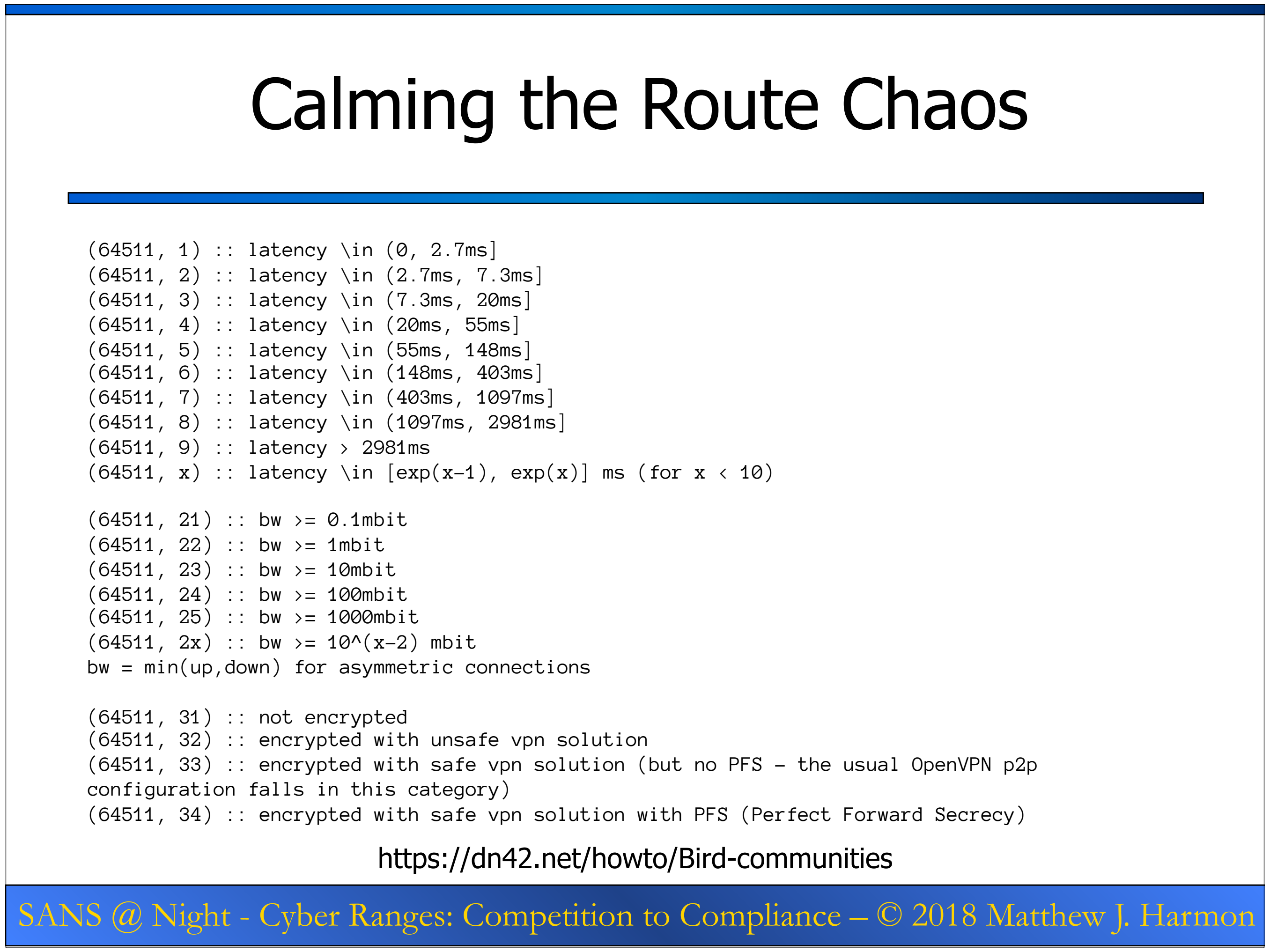
Security Research Network
Chaos Computer Congress
Freinet Germany
AS424242



Routing

- BGP through tinc, FRR
  - tinc chose due to solid history and peer recommendations, sends frequent PING / PONG packets discovering new routes. Perfect for the network edge to discover and add new BGP peers.
- OSPF through WireGuard, BIRD
  - Used as internal protocol as it is quiet and doesn’t send any data when idle. WireGuard formally verified.

The network design as it is today uses BPG at the edge with FRR on OPNsense routing over tinc building an external mesh network, and OSPF over WireGuard internally. WireGuard is very quiet when not in use and the route calculation is performed automatically. We're still experimenting but have had early success simulating some of dn42's services.



Calming the Route Chaos

```
(64511, 1) :: latency \in (0, 2.7ms]
(64511, 2) :: latency \in (2.7ms, 7.3ms]
(64511, 3) :: latency \in (7.3ms, 20ms]
(64511, 4) :: latency \in (20ms, 55ms]
(64511, 5) :: latency \in (55ms, 148ms]
(64511, 6) :: latency \in (148ms, 403ms]
(64511, 7) :: latency \in (403ms, 1097ms]
(64511, 8) :: latency \in (1097ms, 2981ms]
(64511, 9) :: latency > 2981ms
(64511, x) :: latency \in [exp(x-1), exp(x)] ms (for x < 10)

(64511, 21) :: bw >= 0.1mbit
(64511, 22) :: bw >= 1mbit
(64511, 23) :: bw >= 10mbit
(64511, 24) :: bw >= 100mbit
(64511, 25) :: bw >= 1000mbit
(64511, 2x) :: bw >= 10^(x-2) mbit
bw = min(up,down) for asymmetric connections

(64511, 31) :: not encrypted
(64511, 32) :: encrypted with unsafe vpn solution
(64511, 33) :: encrypted with safe vpn solution (but no PFS - the usual OpenVPN p2p
configuration falls in this category)
(64511, 34) :: encrypted with safe vpn solution with PFS (Perfect Forward Secrecy)
```

https://dn42.net/howto/Bird-communities

We've started working with BIRD Communities in order to calm some of the route chaos. In this case, we're able to automatically test for latency and bandwidth and set appropriate community values to optimize traffic flow. Those scripts are in the end slides

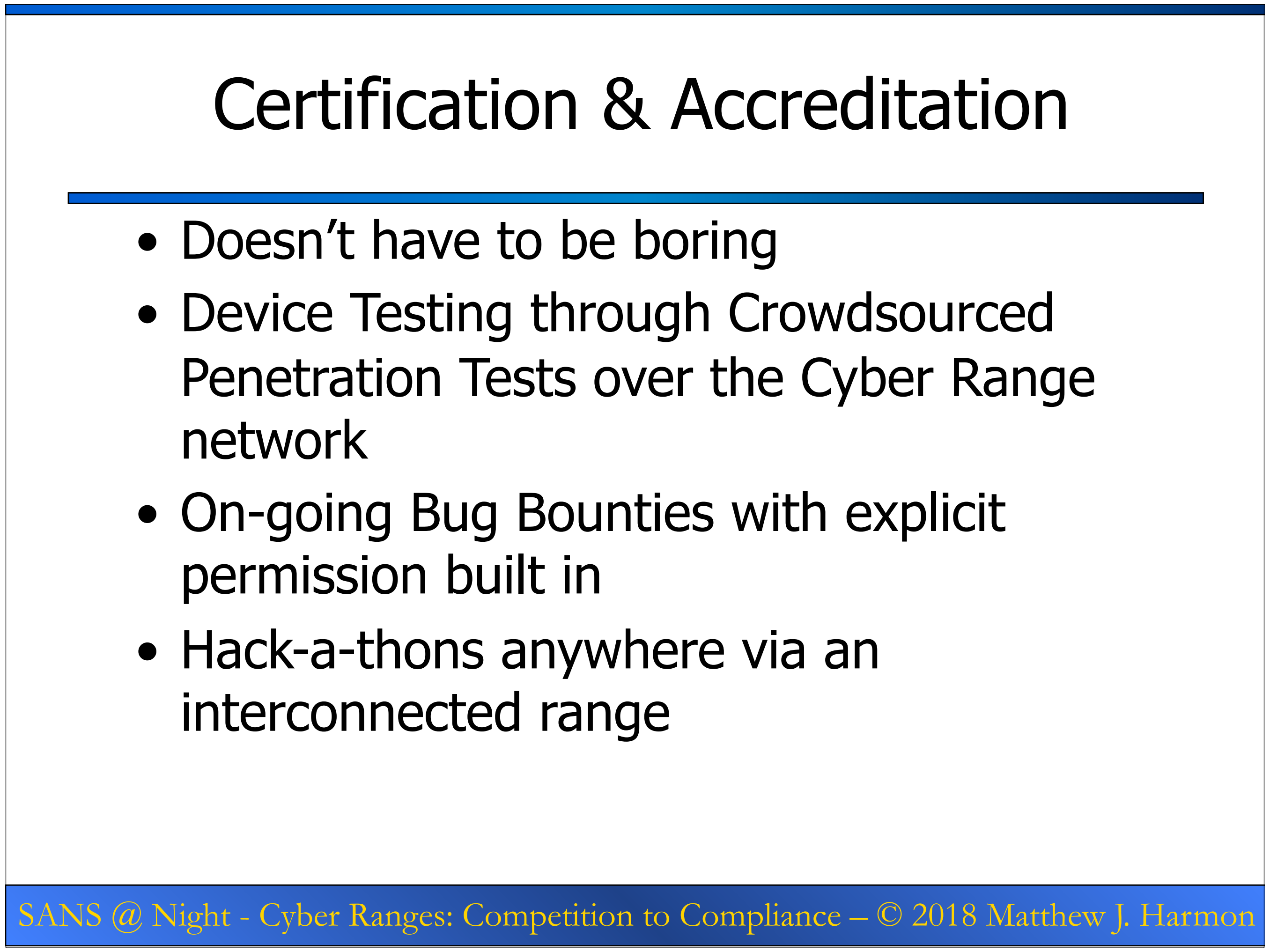
Now that there is a port of WireGuard for HardenedBSD we're looking into using it as our external pipes not just the internal.

My lab data center connection to my closest peer would be : 1, 25, 34

1 - because we both have MICE no more than two hops away

25 - because my lab network has a 1Gig fiber uplink

34 - because we're using encryption with tinc as our link



Certification & Accreditation

- Doesn’t have to be boring
- Device Testing through Crowdsourced Penetration Tests over the Cyber Range network
- On-going Bug Bounties with explicit permission built in
- Hack-a-thons anywhere via an interconnected range

It doesn’t have to be boring!

Cyber Range (Why not?)

- Proper Security Research
- Cyber eSport Competitions
- Corp-to-Corp War Games
- Device Testing & Claim Validation
  - Medical, ICS,
  - Toy Bears, Smart TVs
- Students Writing Malware
- Connect your range to your peers
  - Long distance LAN parties

Shoot for the stars.

Thank you!

matthew@itriskltd.com

IT RISK LIMITED ®

Presentation Repository
https://bit.ly/ITRiskPres

Technology and Business Risk Management,
(Pre-)Audit, Security Testing, Governance,
Interim CISO Services

Sources, References & Credits

1. Colonel Stephanie Horvath US Army MN National Guard
2. JYVSECTEC
3. US Dept of Defense
4. SANS NetWars: https://www.sans.org/netwars/cybercity
5. dn42
    1. BIRD Communities: https://dn42.net/howto/Bird-communities
    2. BIRD Community Latency Script, https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb
6. SpaceX Night Launch, Original Videographer Unknown
7. CrowdSupply, Circumference Raspberry Pi Cluster Project:
    1. https://www.crowdsupply.com/ground-electronics/circumference/
8. YubiKey Configuration
    1. https://github.com/drduh/YubiKey-Guide#4.7-requiring-touch-to-authenticate
    2. https://github.com/Yubico/libu2f-host
    3. https://developers.yubico.com/libu2f-host/Mode_switch_YubiKey.html
9. Lou Ann Jensen
10. David La Belle

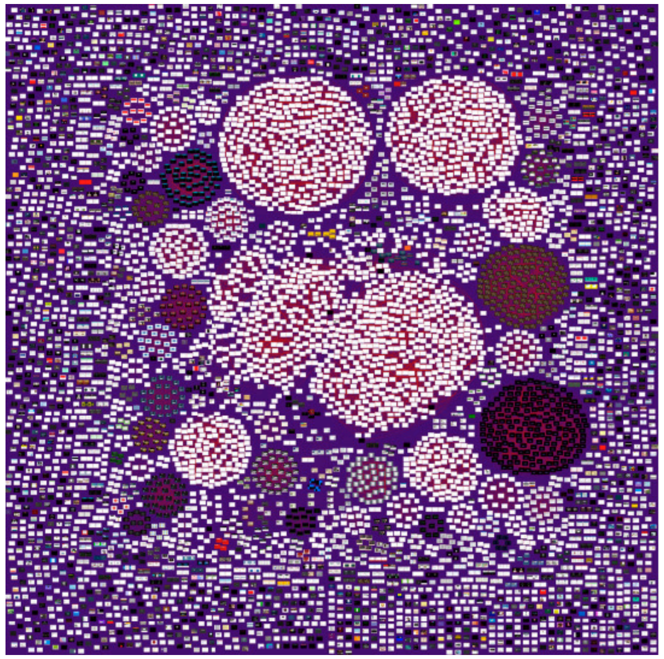
Sources, References & Credits

- Minneapolis Starry Night
- Uber metta
  - https://github.com/uber-common/metta
- MITRE CALDERA
  - https://github.com/mitre/caldera
- https://bsdrp.net/documentation/examples/bgp_route_reflector_and_confederation_using_quagga_and_bird
- https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb
- @HyperionGray Dark Web Map
  - https://blog.hyperiongray.com/dark-web-map-introduction/

Post-Script

- If you’re a network engineer, the previous slides made you think about routing loops and other insanity.
- Introducing BIRD BGP community and automatic calculations.
  - https://bsdrp.net/documentation/examples/bgp_route_reflector_and_confederation_using_quagga_and_bird
  - https://github.com/Mic92/bird-dn42/blob/master/bgp-community.rb

The Dark Web Map by @HyperionGray



https://blog.hyperiongray.com/dark-web-map-introduction/

I’ve heard an InfoSec presentation isn’t proper unless it mentioned the Dark Web. Well, here is HyperionGray’s Dark Web map. We’re not going to explore this, but if you have a chance check it out.