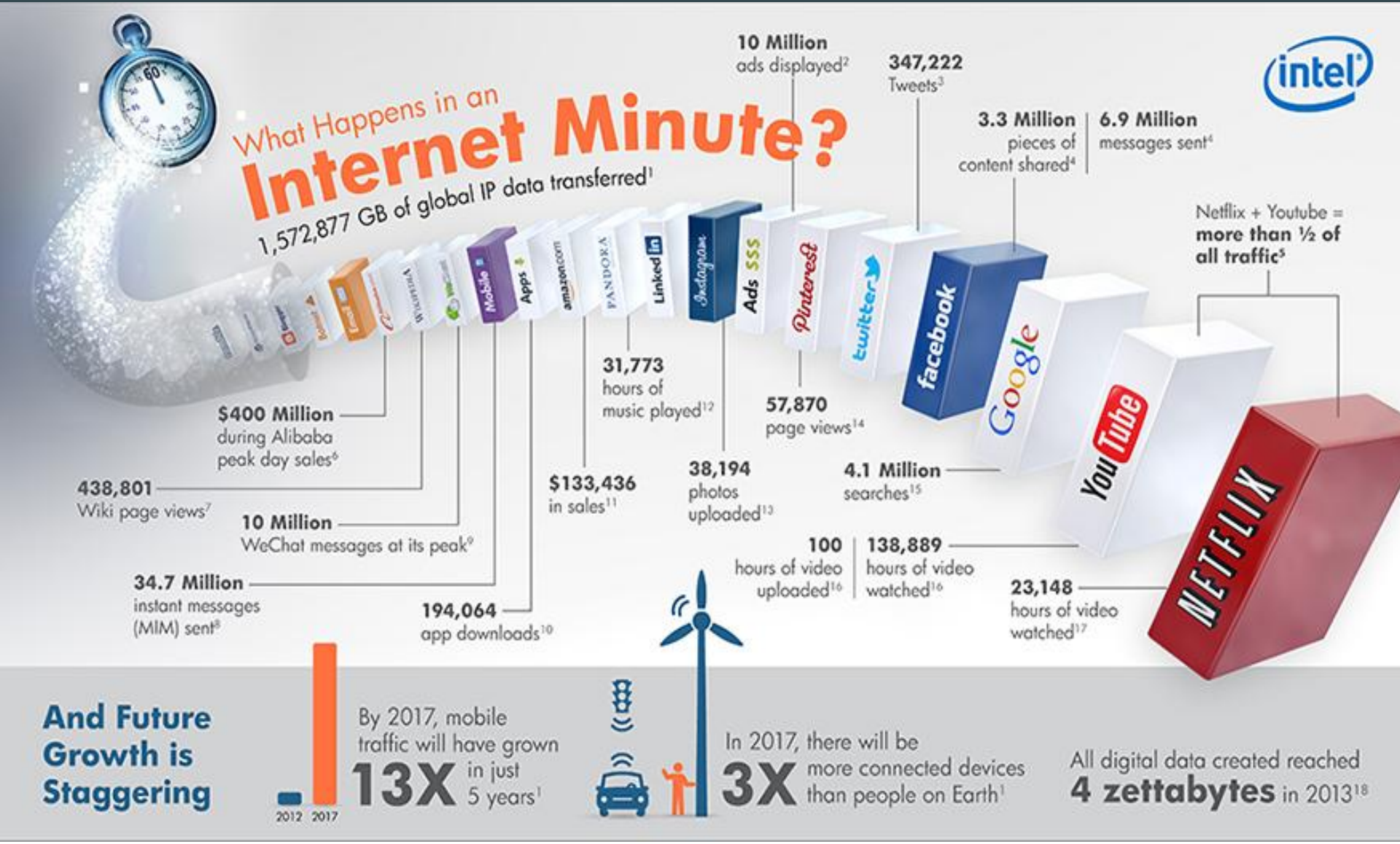
Cyber Security Capacity Building

17 June 2016

Sudipto Jena

The Internet is Ubiquitous: its footprint will only grow!



Source: http://www.intel.in/content/www/in/en/communications/internet-minute-infographic.html

TCG DIGITAL

Crime in the cyber space will only increase, as is evident

Health Insurer Anthem Hit by Hackers

Breach Gets Away With Names, Social Security Numbers of Customers, Employees

By **ANNA WILDE MATHEWS** and **DANNY YADRON**
Updated Feb. 4, 2015 9:39 p.m. ET

Anthem Inc., the country's second-biggest health insurer, said hackers broke into a database containing personal information for about 80 million of its customers and employees in what is likely to be the largest data breach disclosed by a health-care company.

Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab

By Mike Lennon on February 15, 2015

A multinational gang of cybercriminals infiltrated more than 100 banks across 30 countries and made off with up to one billion dollars over a period of roughly two years, Kaspersky Lab said on Saturday.

Pak-based group attack on govt off

PTI | Jun 3, 2016, 08.00 PM IST

New Delhi, Jun 3 () A Pakistan-based group is suspected to be behind cyber attacks on Indian government officials, luring them with emails referencing seventh Central Pay Commission, a software security firm has claimed.

"On May 18, 2016, the group registered a fake news website and sent spear phishing emails to Indian government officials. The emails referenced the Indian government's seventh Central Pay Commission, a topic of interest among officials," security firm FireEye said in a statement.

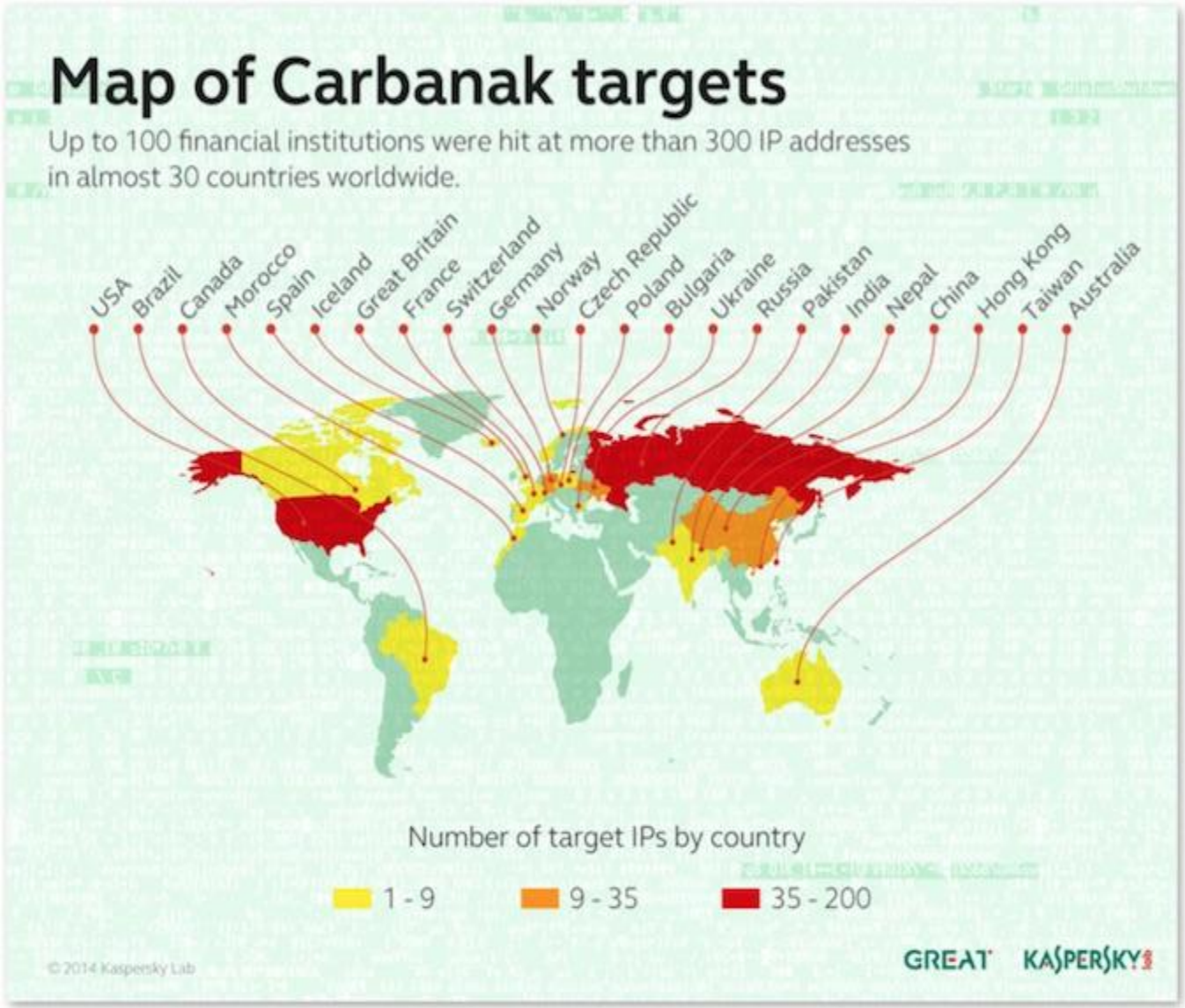
The emails sent to officials were sent from timesofindiaa.in, a fake news domain registered by the attackers, it added.

The group attached a malicious Microsoft Word document to the emails, which pretended to be sent by an employee of a leading publication. They requested the recipient to open the attachment about the seventh Pay Commission.

TCG DIGITAL

Carbanak Malware

Hackers Hit 100 Banks in 'Unprecedented' $1 Billion Cyber Heist: Kaspersky Lab



Interesting Facts

-Attackers used “Spear Phishing” method
- Email attachments used weaponized MS-Word using MSOffice exploits
-After compromise, installed Ammyy Remote Admin Tool
- Ammyy was a preferred tool since many organizations white-listed it for its use with system administrators
- SWIFT network, Oracle Databases, Online banking, ATM machines used

Carbanak is still ACTIVE

TCG DIGITAL

Patch and Pray

A recent C-SPAN interview with Dr. Arati Prabhakar, director of the Defense Advanced Research Projects Agency (DARPA), conducted by Mary Jordon from the *Washington Post,*

"The attacks are happening in microseconds, so today all we can do is patch and pray, and keep throwing **human beings** at the problem."

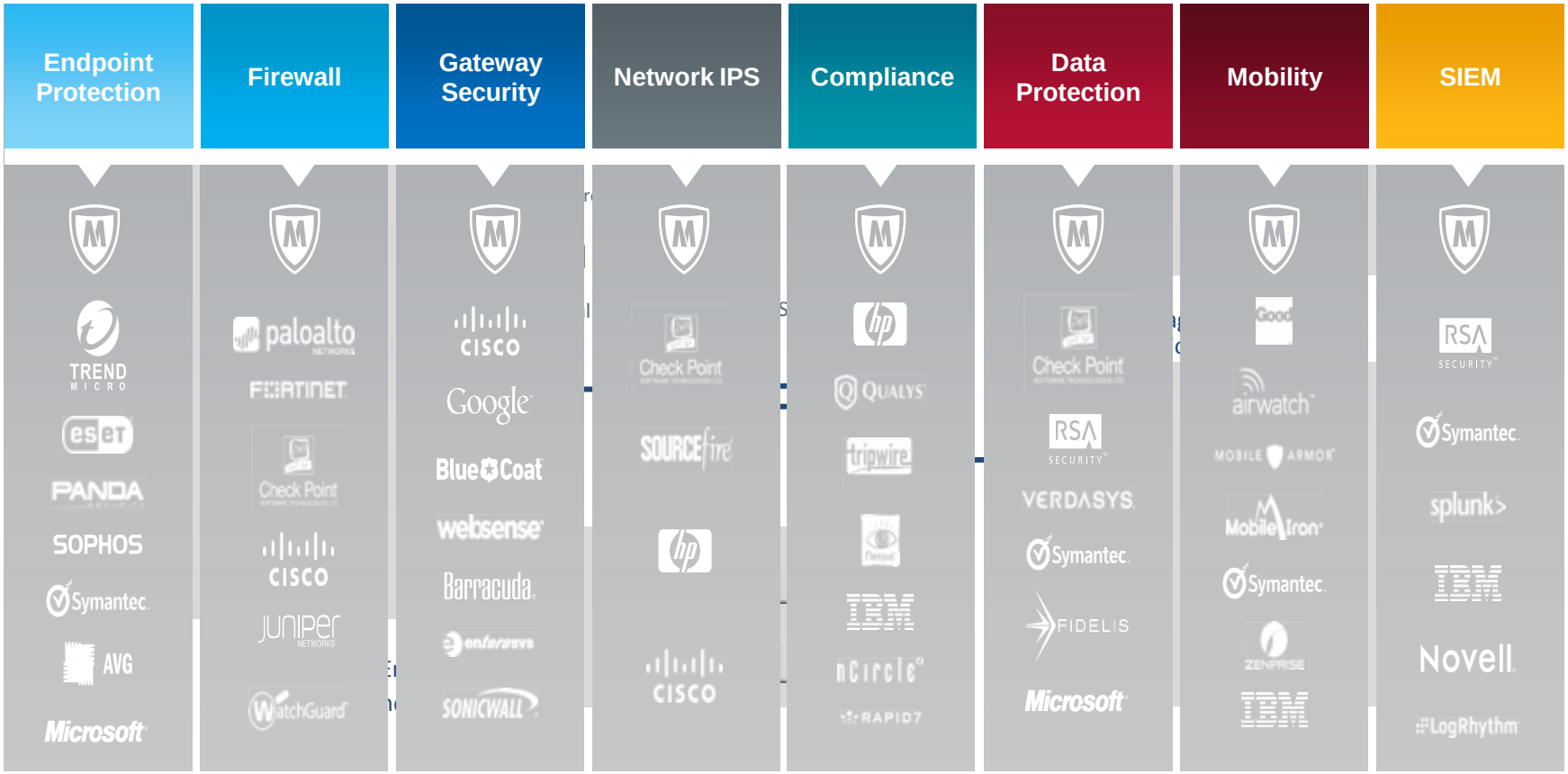
Dr. Arati Prabhakar, director of the DARPA

http://www.govtech.com/dc/articles/DARPA-Director-Calls-for-Cybersecurity-Change.html

TCG DIGITAL

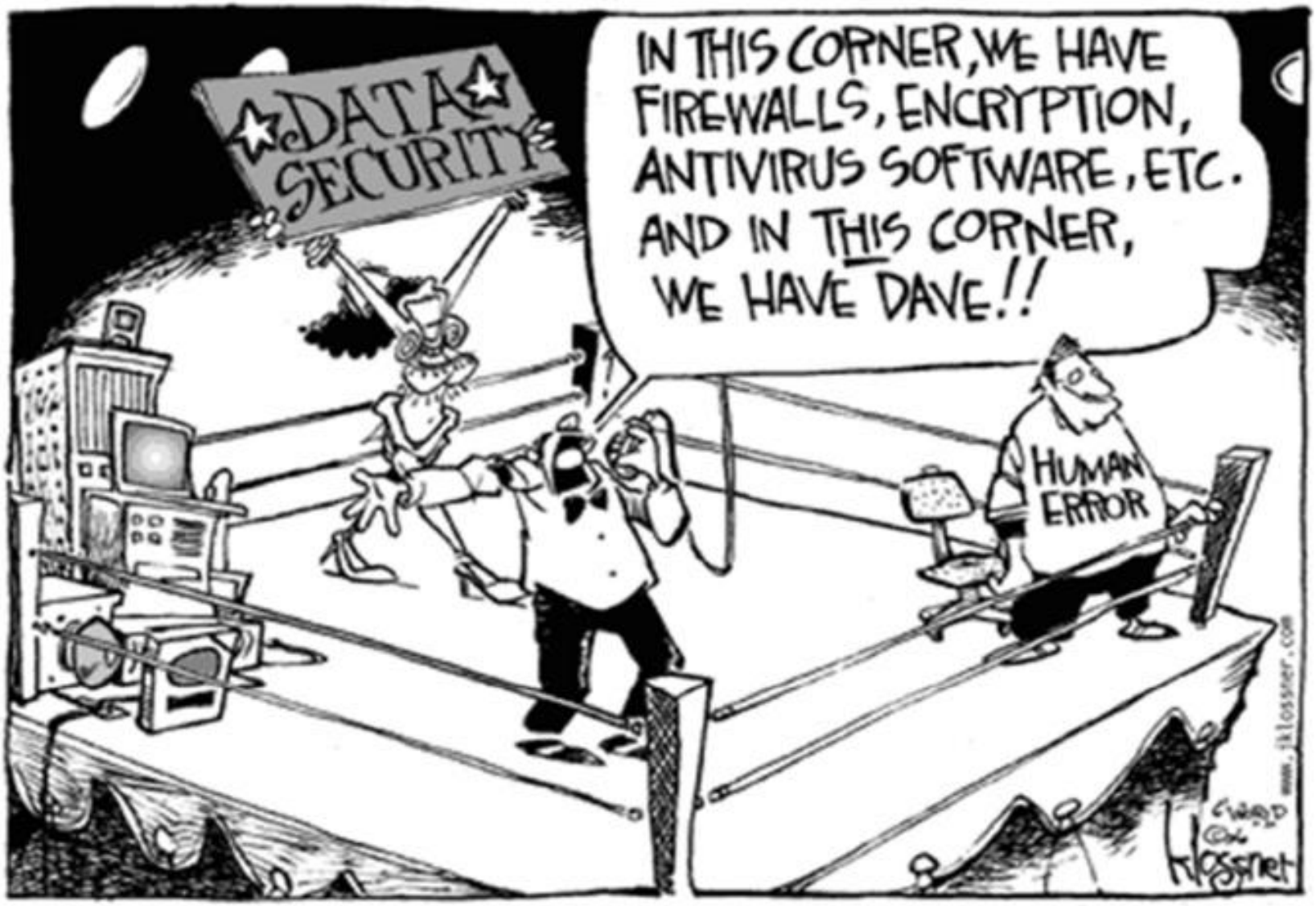
Security Implementation in Silos have Increased

- Deployment in Silos – Higher Cost of Ownership and Scalability
- Numerous Appliances



TCG DIGITAL

In this Cyber-ring of things, there will always be a “Dave”



TCG DIGITAL

…and the traditional counter measures usually deployed

TCG DIGITAL

What is our end goal – rethink strategies

- Learning to be a hacker is not the end objective
- Preventing an attack needs knowledge of device, systems, & their operations
- Training required for expertise on network security – how to be pro-active?

Hackers are now professionals not school kids

Copyright © 2015 TCG Digital Solutions. All Rights Reserved.

TCG DIGITAL

Expectations from next generation defenders

- Ability to isolate issues - deep understanding of the Internet is a pre-requisite
- How to identify attacks from within the swarm of Internet Cloud?
- Eliminating attacks while maintaining traffic continuity

Co-ordinated Response to Particular Incidents is what is required

With the rise cyber crime it is important to ponder on some questions

How do you learn about new threats?

Is your training only vendor specific?

Is the training organizationally relevant ?

How do you respond to an incident?

Are you ready to work as a TEAM while responding to an incident?

TCG DIGITAL

How to build technical cyber capabilities

- Hardware Skills
- Operating system skills
- Server skills
- Linux/Windows/Apple skills
- Networking skills
- Foundational Security skills
- Generalists Security skills
- Specialist Security skills
  - Penetration Testing
  - Network Defence
  - Incident Handling
  - Forensic Analysts
  - Security Control Assessors

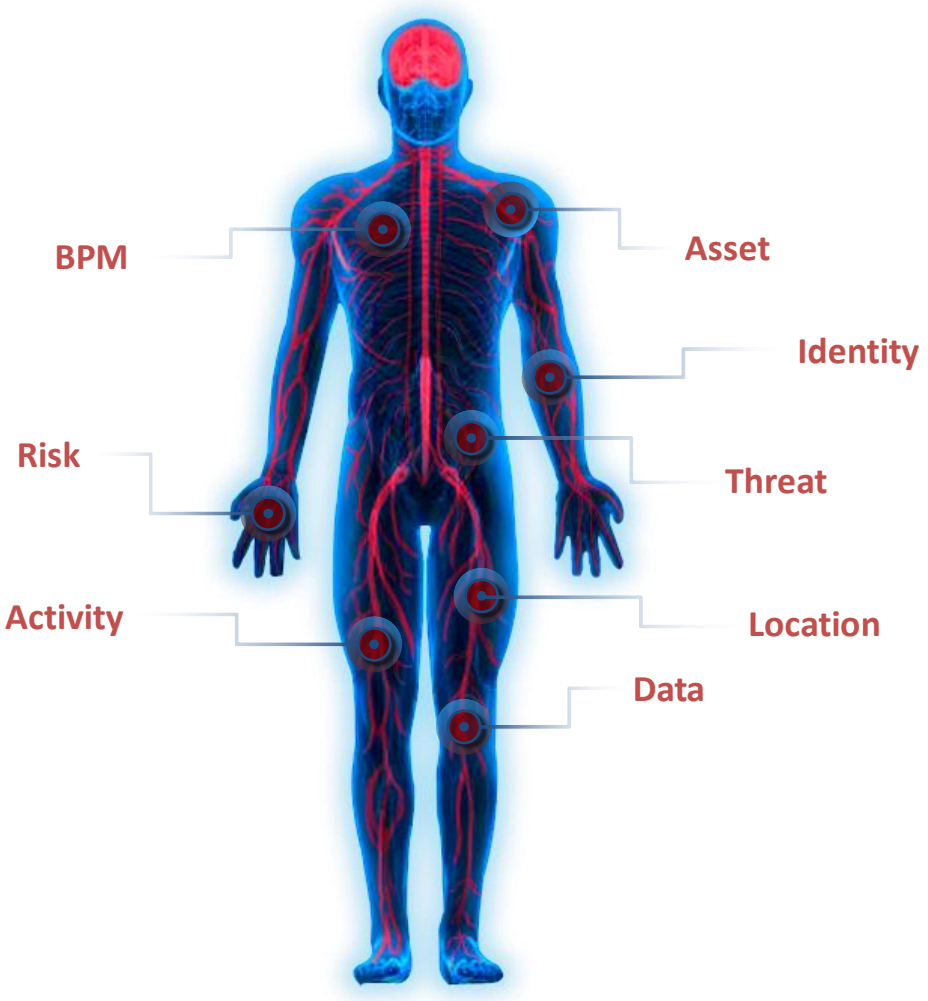


Image courtesy: McAfee

How do you move from Individual to a Team Sport

Cyber Maturity

Emphasis on Training

Hands-on Environment

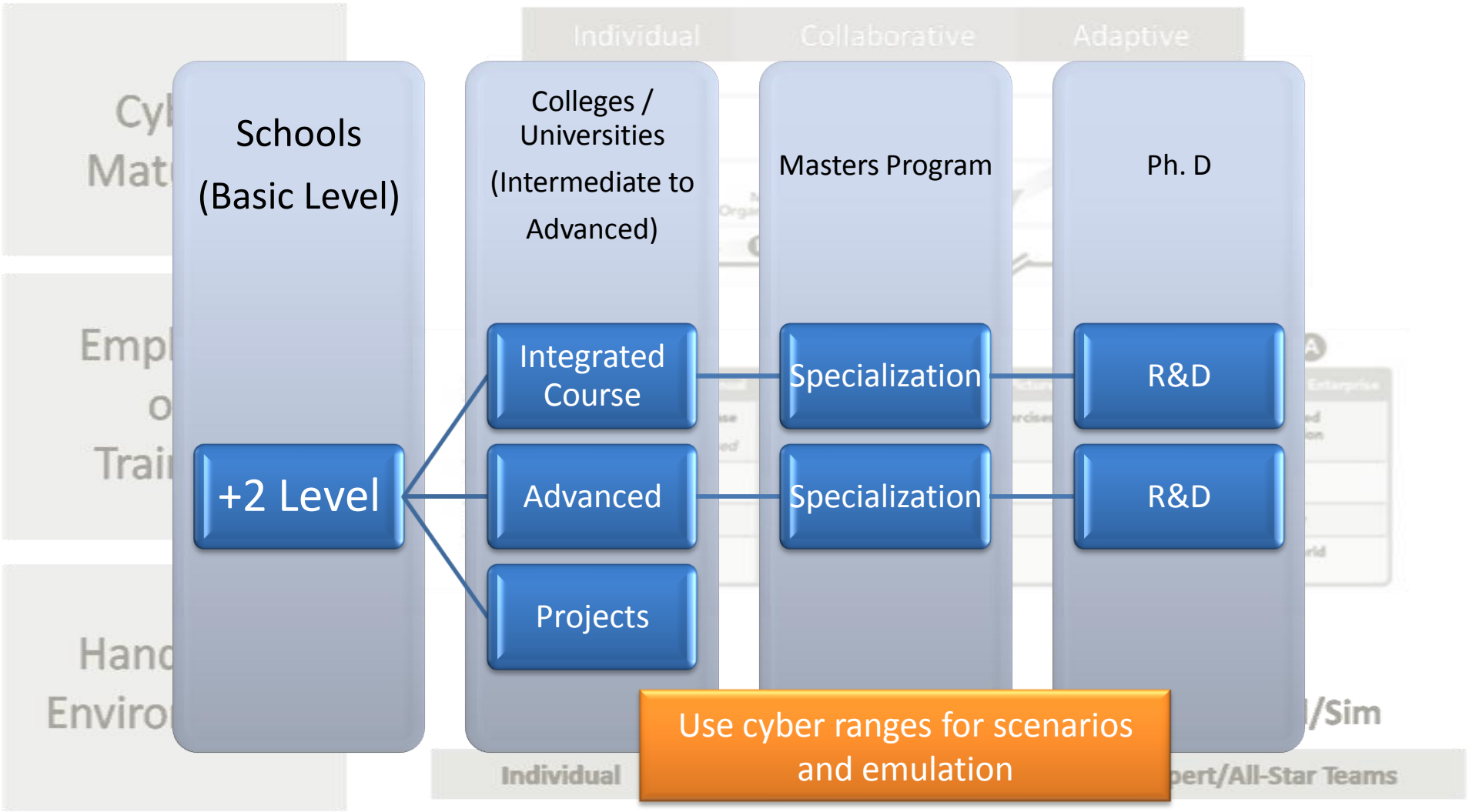
	E	D	C	B	A
MATURITY LEVEL	Reactive & Manual	Tools Level	Integrated Picture	Dynamic Defence	Resilient Enterprise
TRAINING *INSTRUCTION*	Knowledge Base *Classroom Based*	Cyber Challenges *Hands-on Lab*	Dynamic Exercises *Facilitated*	Modeling & Simulation	Advanced Simulation
COMPETENCY	Basic	Intermediate	Advanced (Custom)	Advanced (Scenario Based)	Expert
PROFICIENCY	Baseline	Individual	Team	Organizational	Mastery
ENVIRONMENT	Standard	Standard/ Customized	Customized	Customized/ Real World	Real World

Basic → Intermediate → Advanced → Mod/Sim

Individual | Team | Specialist/Good Teams | Expert/All-Star Teams

TCG DIGITAL

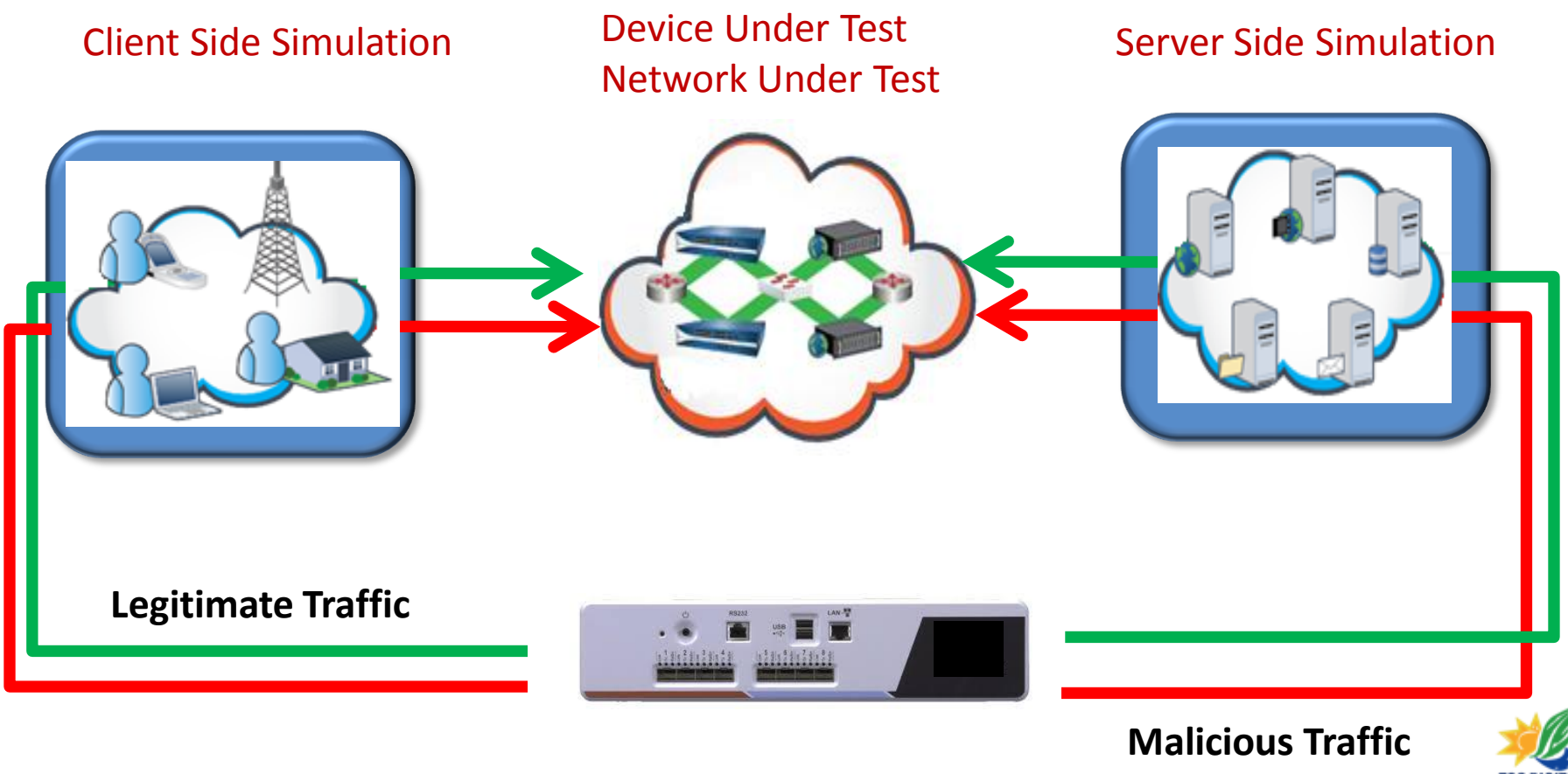
Integrate ICT security in curriculum



Logical view of the cyber range

Simulate legitimate user communications, using more than 200+ applications. Harden network resiliency to both recreational and malicious traffic

Simulate malicious users sending malicious traffic using more than 38000+ attacks including live malware



Source: McAfee Labs

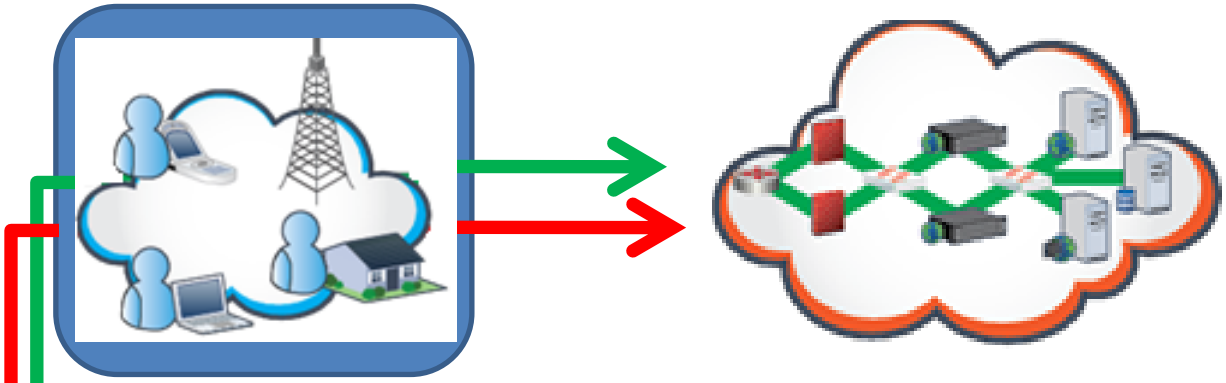
Logical Network Setup Using Cyber-Range

Validate current cyber security test methodologies to validate future performance of your Firewalls, IPS, Servers etc

Identify the potential limits of and vulnerabilities of current network infrastructure and optimize its performance

Client Side Simulation

Server Under Test
Service Under Test



Legitimate Traffic

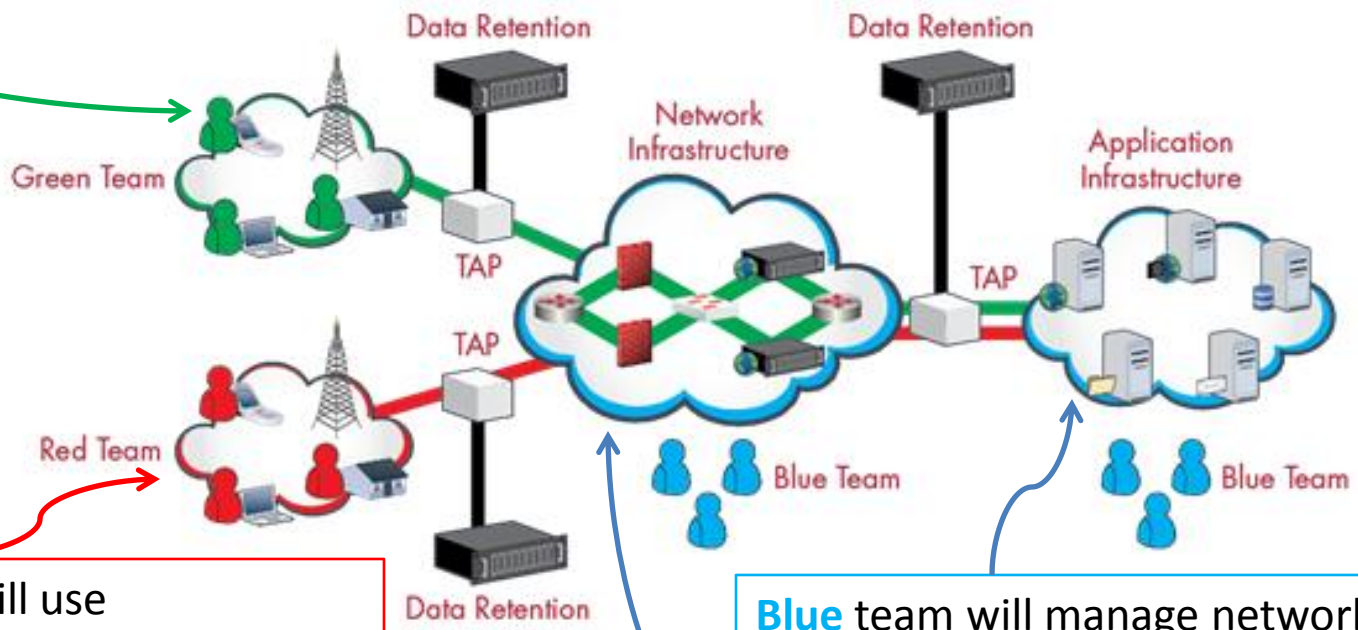
Malicious Traffic

Source: McAfee Labs

TCG DIGITAL

Logical Network Setup Using Cyber-Range

Green team will use PerfectStorm to simulate users and "good" traffic accessing applications Hosted on network infrastructure managed by **Blue** Team.



Red team will use PerfectStorm to simulate malicious users sending malicious traffic such as network attacks, and spywares to the network infrastructure managed by **Blue** Team.

Blue team will manage network infrastructure using FW/NGFW and hosting web servers, anti-virus, application servers, HIDS, HIPS etc within a virtualized or physical devices.

Source: McAfee Labs

TCG DIGITAL

Cyber Architecture – Use Hybrid Architecture

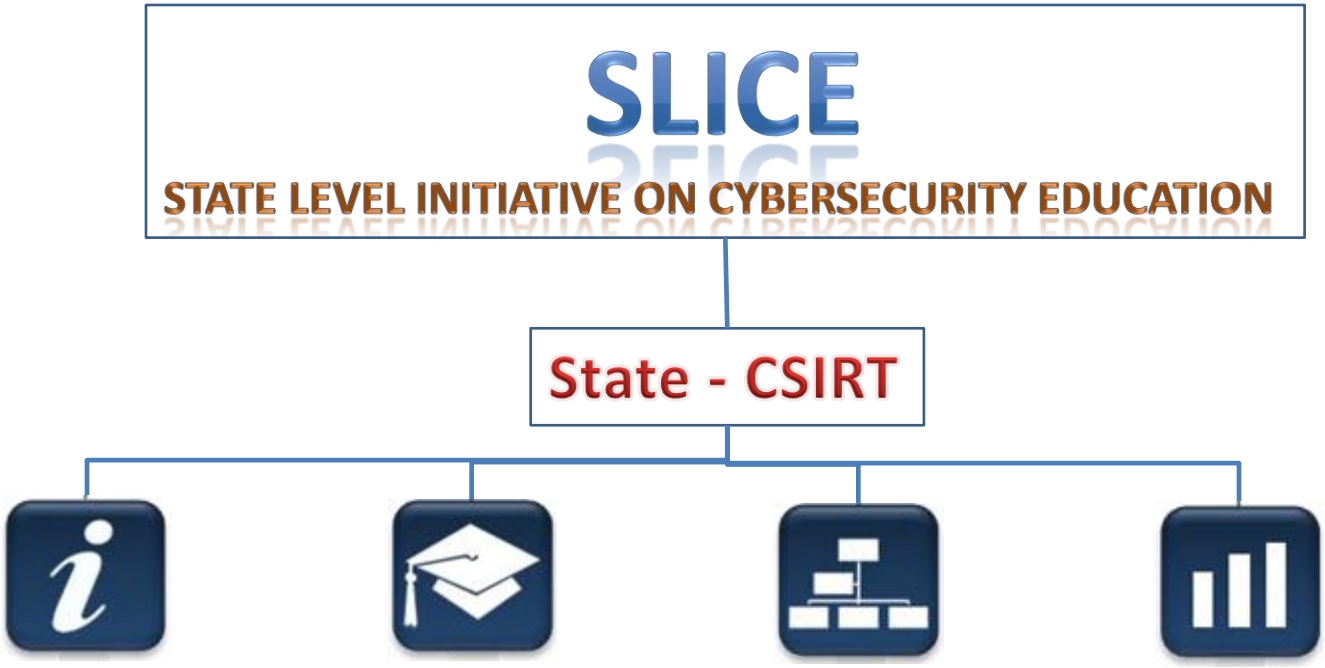
A hybrid architecture utilizes **virtual** elements where it makes sense and **physical** elements when and where they make sense.

- **Virtualize:** Windows and Linux Servers, workstations, some network switching and routing
- **Physical:** Video-Surveillance camera, network printers, VOIP, Security Equipment, networks and routing
- Using actual security equipment in your range environment is an essential condsideration, such as mimicking whatever FW/IPS/IDS you use in production, since it is **impossible** to virtualize these with any degree of realism.

Source: McAfee Labs

TCG DIGITAL

S.L.I.C.E. – State Level Initiative on Cyber Security Education



Component 1
State Cybersecurity Awareness

Component 2
Formal Cybersecurity Education

Component 3
Cybersecurity Workforce Structure

Component 4
Cybersecurity Workforce, Training and Professional Development

S.L.I.C.E. – State Level Initiative on Cyber Security Education

SECURELY PROVISION - responsible for conceptualizing, designing, and building secure information technology (IT) systems

OPERATE & MAINTAIN - responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security

PROTECT & DEFEND - responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks

INVESTIGATE - responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence

COLLECT & OPERATE - responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence

ANALYZE - responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence

OVERSIGHT & DEVELOPMENT - providing leadership, management, direction, and/or development and advocacy

TCG DIGITAL

The Age of the **Possible**

Computing advances will **advance human progress at an unprecedented rate**. From medicine and science to e-commerce and education, we are seeing astounding changes.

Technology can enable global connections to a degree once thought impossible – but it all happens only if we are **assured that the computing environment is safe.**

Security has never been more necessary, and now it has a dual purpose – **to enable as well as defend**.

The opportunities to **Explore, Connect, Build, and Cure** are too great to be hindered by **Fear**.

TCG DIGITAL

Thank you

joydeep.bhattacharya@tcg-digital.com