Developing a Network Defense course

T. Andrew Yang

Dept. of Computing Sciences

University of Houston-Clear Lake

yang@uhcl.edu

Outline

- Background information
- Motivation
- Design approach
- Objectives
- Learning outcomes
- Course structure: modules, submodules, course units
- Lessons learned

What is *cyberspace*?

cyber

“of, relating to, or involving computers or computer networks (such as the Internet)” (Merriam-Webster)

e.g., cyberspace, cybercrime, cyberwar, cyberbullying, cyberterrorists, the cyber marketplace

cyberspace

“the online world of computer networks and especially the Internet” (Merriam-Webster)

What is *cyberspace*?

- *Military perspective*

  (*JP 3-12 Cyberspace Operations*, DoD Joint Publications, June 2018)

  “A <u>global</u> domain within the information environment consisting of the interdependent <u>networks</u> of information technology infrastructures and resident <u>data</u>, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”

What is *cyberspace*? (per JP 3-12)

Although cyberspace coexists with the other domains, it is a separate domain.

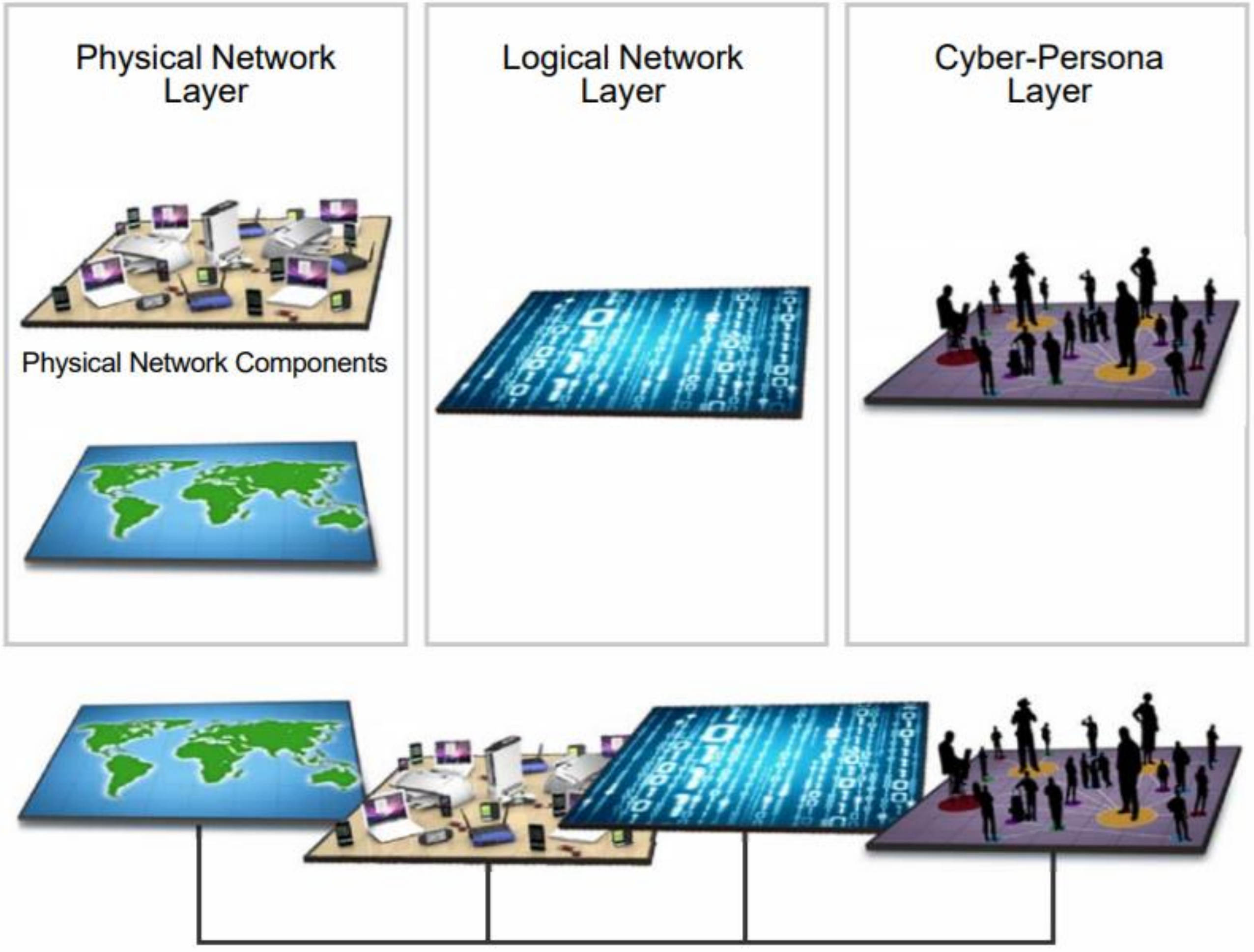
Cyberspace pervades the land, air, maritime, and space domains through the EMS and wired networks.

Cyberspace enables integration across physical domains by moving data along transmission paths through links and nodes in cyberspace and the EMS.

The man-made aspects of cyberspace, coupled with continual advances in technologies, contribute to a continuous obligation to manage risk and protect portions of cyberspace.

- Source: *JP 3-12 Cyberspace Operations*, DoD Joint Publications, 8 June, 2018

The Three Interrelated Layers of Cyberspace



Distinct, Yet Interrelated

Source: *DoD FM 3-12 Cyberspace and Electronic Warfare Operations*, DoD, April 2017

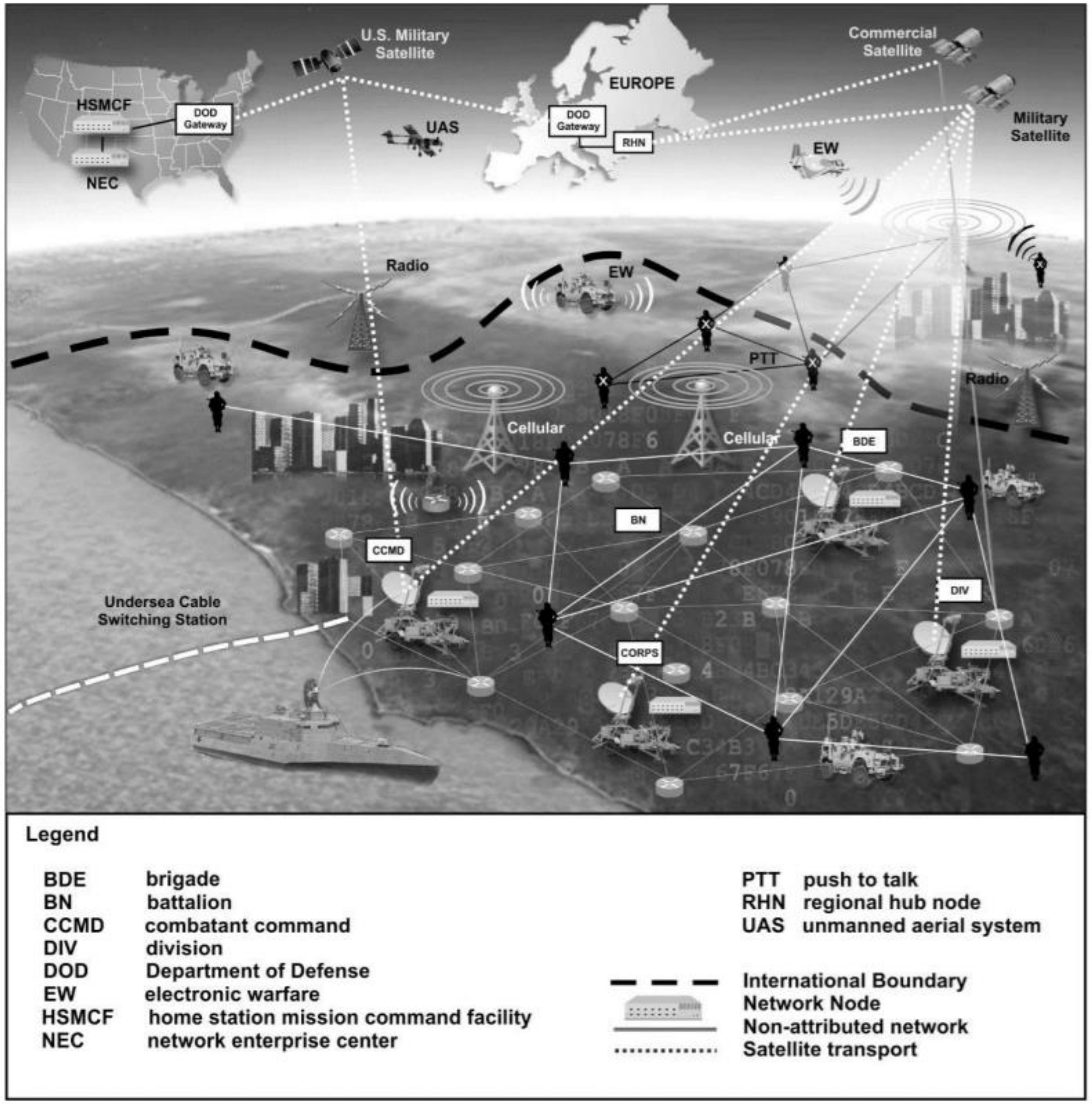


Figure 1-1. Visualization of cyberspace and the electromagnetic spectrum in an operational environment

Motivation

- To develop an undergraduate Network Defense course that meet the NSA/DHS designation requirements for the Center of Academic Excellence (CAE) in Cyber Defense Education (CAE-CDE)

+ integrated hands-on experience

- Three types of CAEs in Cyber Defense
  - CAE-2Y
  - CAE-CDE
  - CAE-R

Knowledge Units (KUs)

- To qualify for one of the CAE designations, institutions must ensure their programs are closely aligned with specific cybersecurity-related **knowledge units**, validated by experts in the field.
- Programs must include core knowledge units (KUs) on specific topics of study.

KUs required of the *CAE-2Y programs*

- Basic Data Analysis
- Basic Scripting or Introductory Programming
- Cyber Defense
- Cyber Threats
- Fundamental Security Design Principles
- IA Fundamentals
- Intro to Cryptography
- IT Systems Components
- Networking Concepts
- Policy, Legal, Ethics, and Compliance
- System Administration

KUs required of the ***CAE-CDE programs***

- The KUs of CAE-2Y programs, plus the following:
    - Databases
    - ✓Network Defense
    - Networking Technology and Protocols
    - Operating Systems Concepts
    - Probability and Statistics
    - Programming

Outline

- Background information
- Motivation

➢Design approach

- Objectives
- Learning outcomes
- Course structure: modules, submodules, course units
- Lessons learned

KU in Network Defense (NDF)

Source: https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

- **Intent:** to provide students with knowledge of the concepts used in defending a network, and the basic tools and techniques that can be taken to protect a network and communication assets from cyber threats.

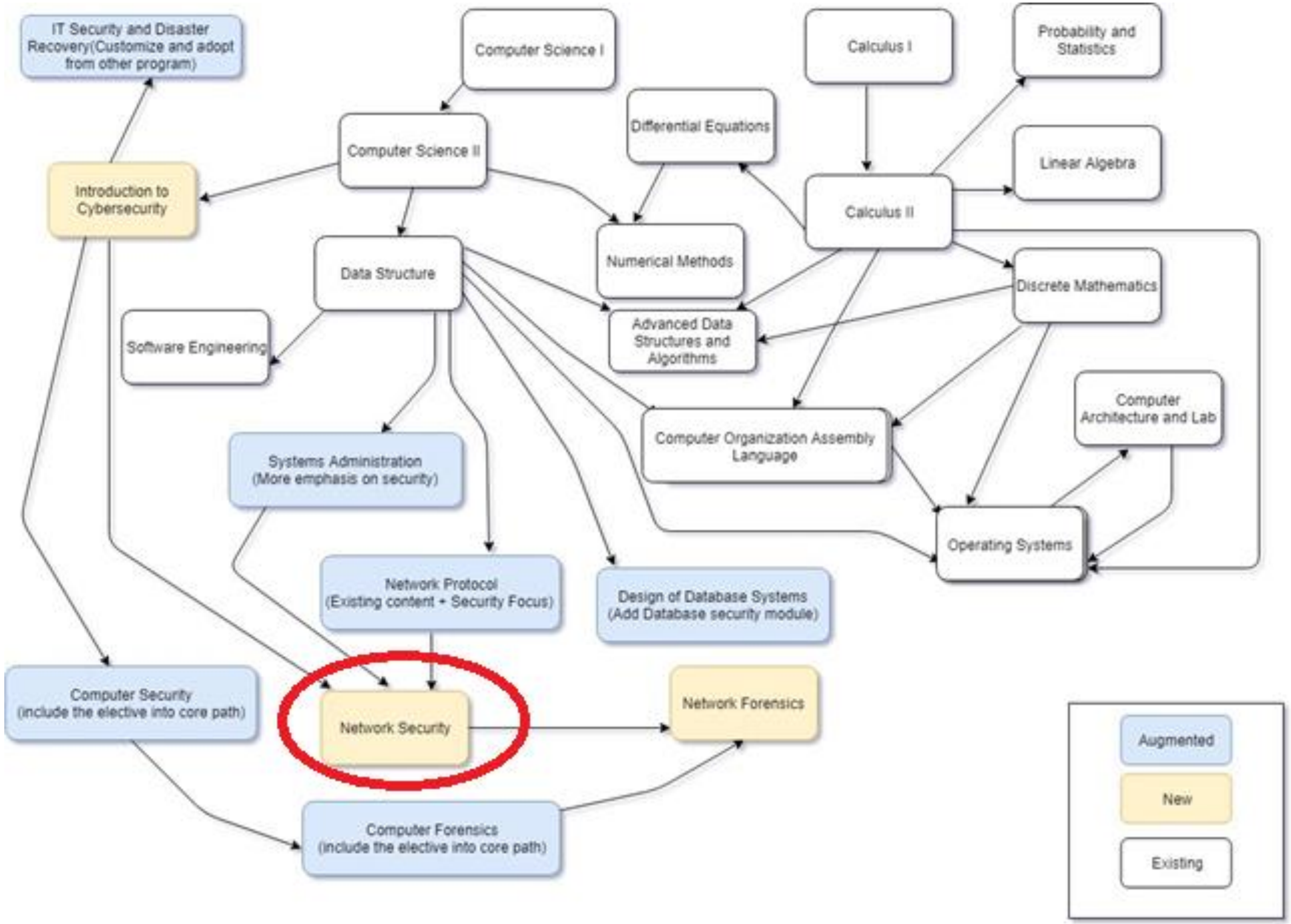
- **Four Topic Areas**

1. Essential concepts of network defense, such as:
    - Defense in Depth
    - Network attacks
    - Network Hardening
    - Minimizing Exposure (Attack Surface and Vectors)

KU in Network Defense (NDF)

2. Network defense/monitoring tools:
    - Implementing Firewalls
    - DMZs / Proxy Servers
    - VPNs
    - Honeypots and Honeynets
    - Implementing IDS/IPS
3. Network Operations:
    - Network Security Monitoring
    - Network Traffic Analysis
4. Network security policies as they relate to network defense/security:
    - Network Access Control (internal and external)
    - Network Policy Development and Enforcement

Prerequisite Chart


IT Security and Disaster Recovery(Customize and adopt from other program)
Computer Science I
Calculus I
Probability and Statistics
Computer Science II
Differential Equations
Linear Algebra
Introduction to Cybersecurity
Calculus II
Data Structure
Numerical Methods
Discrete Mathematics
Software Engineering
Advanced Data Structures and Algorithms
Computer Architecture and Lab
Systems Administration (More emphasis on security)
Computer Organization Assembly Language
Operating Systems
Network Protocol (Existing content + Security Focus)
Design of Database Systems (Add Database security module)
Computer Security (include the elective into core path)
Network Security
Network Forensics
Computer Forensics (include the elective into core path)
Augmented
New
Existing

Learning outcomes

- The student, after having successfully completed the class, should be able to
  1. Understand fundamental security issues in computer networks
  2. Understand the common mechanisms used in securing a network
  3. Design a TCP/IP network with IP Security
  4. Design and deploy firewalls to secure a private network
  5. Design and deploy a virtual private network to secure remote connections
  6. Select appropriate methods to detect and counter intrusions to a network
  7. Understand other advanced issues related to network security

Course structure

Module 1: Network Defense Basics and Principles

Submodule 1 – Network Security Basics

Submodule 2 – Defense Principles

Module 2: Network Defense Mechanisms

Submodule 3 – Network Defense Mechanisms (part 1)

Submodule 4 – Network Defense Mechanisms (part 2)

Module 3: Policy, Operation, and Assurance

Module 4: Network Defense Hands-on activities

Module 1: Network Defense Basics and Principles

- Submodule 1 – Network Security Basics
  - Unit ND_1: Introduction to Network Security (Review of the OSI Network Reference Model, IP Addressing)
  - Unit ND_2: Network Attacks (e.g., session hijacking, Man-in-the-Middle)
  - Unit ND_3: DNS and attacks
  - Unit ND_4: Cryptography
  - Unit ND_5: Security Services (Confidentiality, Data integrity, Origin integrity, Availability, and Non-Repudiability)
- Submodule 2 – Defense Principles
  - Unit ND_6: Network Defense Principles (Minimizing Exposure, Defense in Depth)

Module 2: Network Defense Mechanisms

- Submodule 3 – Network Defense Mechanisms (part 1)
  - Unit ND_7: Network Access Control (internal and external)
  - Unit ND_8: Firewalls, Proxy Server
  - Unit ND_9: Implementing Firewall, DMZs
  - Unit ND_10: Application-layer security: HTTPS
  - Unit ND_11: Network-layer security: IPSec

- Submodule 4 – Network Defense Mechanisms (part 2)
  - Unit ND_12: Implementing IDS/IPS
  - Unit ND_13: Network Monitoring
  - Unit ND_14: Honeypots and Honeynets
  - Unit ND_15: Network Traffic Analysis

Module 3: Policy, Operation, and Assurance

- Unit ND_16: Network Policy Development and Enforcement
- Unit ND_17: Network Operational Procedures
- Unit ND_18: Mission Assurance

Module 4: Network Defense Hands-on activities

- Utilized some of the labs in the SEED Labs

- Five Take-home labs
  - *Local DNS Attack* lab
  - *Firewall Exploration Lab*
  - *Heartbleed Attack Lab*
  - *TCP/IP Attack Lab*
  - *Packet Sniffing and Spoofing Lab*

- Two In-class labs
  - Public Key Infrastructure (PKI) and Man-in-the-middle attacks Lab
  - TBD - prob. Virtual Private Networks (VPN) lab

Outline

- Background information
- Motivation
- Design approach
- Objectives
- Learning outcomes
- Course structure: modules, submodules, course units

➢ Lessons learned

Lessons learned

1. Integrating pre-developed network and computer security labs saves instructors time.

   However, adopting the labs requires either the instructor him/herself or a student assistant to run through the labs beforehand.

2. Covering all the listed topics in the Network Defense knowledge unit could be challenging, in particular when the enrolled students may not all have the prerequisite knowledge.

Questions / Comments ?

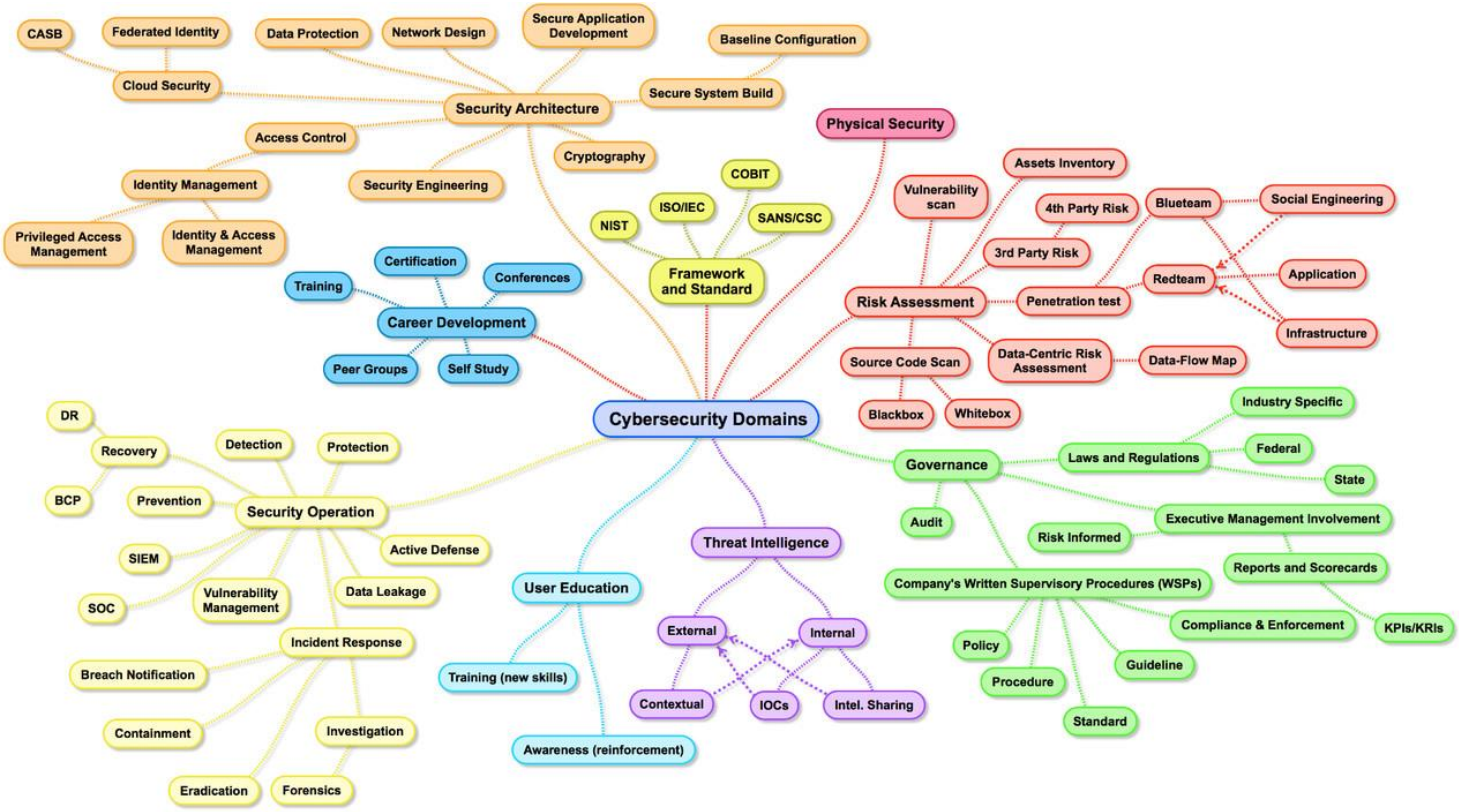
Andrew Yang

yang@uhcl.edu

Cybersecurity domains (aka. The World of Cybersecurity Map)

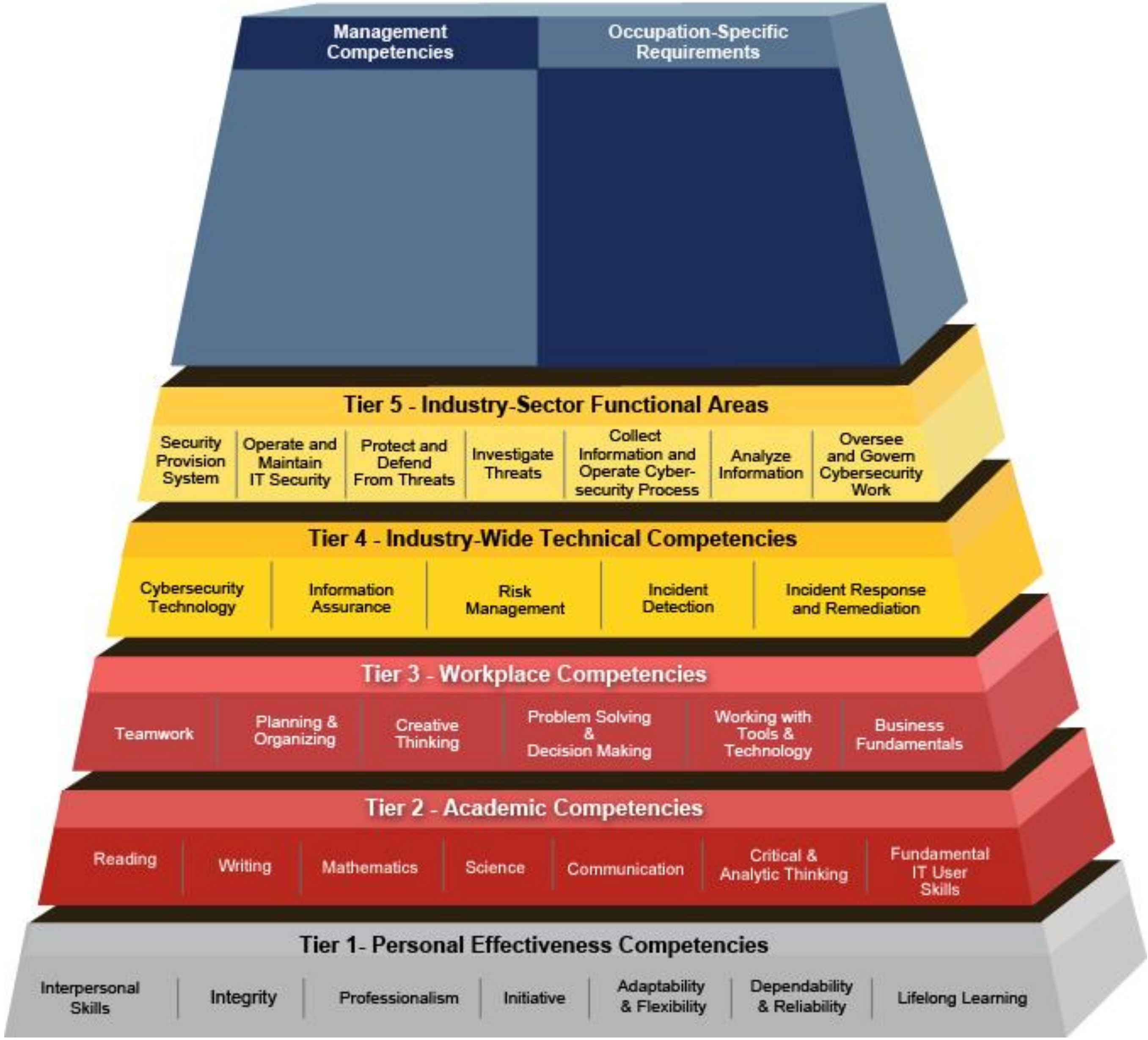
source: https://2.bp.blogspot.com/-OgGmvicsBPk/WNEl5_R2xpI/AAAAAAAAfvQ/gFEk1qkhaT805_R4MBzcc7MtjaNm2-YRACLcB/s1600/cybersecurity%2Bdomains%2Bv2-0%2Bhenry%2Bjiang.png

originally published by Henry Jiang at https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/.



- Cybersecurity Domains
  - Security Architecture
    - Cloud Security
      - CASB
      - Federated Identity
    - Data Protection
    - Network Design
    - Secure Application Development
    - Secure System Build
      - Baseline Configuration
    - Access Control
      - Identity Management
        - Privileged Access Management
        - Identity & Access Management
    - Security Engineering
    - Cryptography
  - Framework and Standard
    - NIST
    - ISO/IEC
    - COBIT
    - SANS/CSC
  - Physical Security
  - Risk Assessment
    - Vulnerability scan
    - Assets Inventory
    - 3rd Party Risk
      - 4th Party Risk
    - Penetration test
      - Blueteam
      - Redteam
        - Social Engineering
        - Application
        - Infrastructure
    - Data-Centric Risk Assessment
      - Data-Flow Map
    - Source Code Scan
      - Blackbox
      - Whitebox
  - Career Development
    - Training
    - Certification
    - Conferences
    - Peer Groups
    - Self Study
  - Governance
    - Laws and Regulations
      - Industry Specific
      - Federal
      - State
    - Executive Management Involvement
    - Risk Informed
    - Reports and Scorecards
      - KPIs/KRIs
    - Audit
    - Company's Written Supervisory Procedures (WSPs)
      - Policy
      - Procedure
      - Standard
      - Guideline
    - Compliance & Enforcement
  - Threat Intelligence
    - External
    - Internal
    - Contextual
    - IOCs
    - Intel. Sharing
  - User Education
    - Training (new skills)
    - Awareness (reinforcement)
  - Security Operation
    - Recovery
      - DR
      - BCP
    - Detection
    - Protection
    - Prevention
    - Active Defense
    - SIEM
    - SOC
    - Vulnerability Management
    - Data Leakage
    - Incident Response
      - Breach Notification
      - Containment
      - Eradication
      - Investigation
      - Forensics

https://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx



Management Competencies

Occupation-Specific Requirements

Tier 5 - Industry-Sector Functional Areas

- Security Provision System
- Operate and Maintain IT Security
- Protect and Defend From Threats
- Investigate Threats
- Collect Information and Operate Cyber-security Process
- Analyze Information
- Oversee and Govern Cybersecurity Work

Tier 4 - Industry-Wide Technical Competencies

- Cybersecurity Technology
- Information Assurance
- Risk Management
- Incident Detection
- Incident Response and Remediation

Tier 3 - Workplace Competencies

- Teamwork
- Planning & Organizing
- Creative Thinking
- Problem Solving & Decision Making
- Working with Tools & Technology
- Business Fundamentals

Tier 2 - Academic Competencies

- Reading
- Writing
- Mathematics
- Science
- Communication
- Critical & Analytic Thinking
- Fundamental IT User Skills

Tier 1- Personal Effectiveness Competencies

- Interpersonal Skills
- Integrity
- Professionalism
- Initiative
- Adaptability & Flexibility
- Dependability & Reliability
- Lifelong Learning