SY110
Intro to Cyber Security

Major Brian Hawkins, USMC

U.S. Naval Academy

Fall AY 2018

Outline

1. Introductions

2. Getting started
   - Admin
   - Why care about Cyber Security?
   - Course Organization

3. Cyber Domain

Introductions

Around the room...

- Things to share:
  - Name, Company
  - Where you're from
  - Planned major
  - Varsity athlete?
  - Prior enlisted military?
  - Service selection thoughts?
  - CS/IT/Cyber background, if any
  - Anything else interesting about yourself you'd like to share

A little about myself

Contact info

- Major Brian Hawkins, USMC
- Office – Michelson 326
- Email – bhawkins@usna.edu
- Phone – x3-6572
- Office hours – Walk-in or by appointment

Who I am

- MOS
  - CH-46E Pilot
  - Data Systems Specialist
  - Acquisition Candidate
  - WTI (AGS)
- Education
  - Education – B.S. Computer Science, USNA, '01
  - M.S. Computer Science, NPS, '09

Admin

- Section Leader/Assistant Section Leader
- Attendance
- Required Software/Computer Issues?
- Course Policies
  - `http://rona.academy.usna.edu/~sy110/info/course-policy.pdf`
  - `http://faculty.cs.usna.edu/~bhawkins/courses/sy110/docs/course_policy_supplement/course_policy.pdf`
- Course Webpages
  - SY110 Course Website: `http://rona.academy.usna.edu/~sy110`
  - My lecture material: `http://http://faculty.cs.usna.edu/~bhawkins/courses/sy110/`
  - Message board `http://rona.academy.usna.edu/~bhawkins/msg/mb.html`
  - Bookmark these!
- Guest Lectures

Why care about Cyber Security?

Why care about Cyber Security?

Recent cyber security examples in the news

- Stuxnet
- Sony hack
- OPM data breach
- Chinese gov’t monitoring of US gov’t email
- Others?

Why care about Cyber Security?

Recent cyber security examples in the news

- Stuxnet
- Sony hack
- OPM data breach
- Chinese gov't monitoring of US gov't email
- Others?

Why should DoD/DoN/USNA care?

3 Focus Areas of SY110

Cyber Battlefield

- Basic components of “cyberspace”
  - What are they?

Cyber Security Tools

- Tools and strategies used to protect ourselves against attack, and attack adversary networks
  - *e.g.* firewalls, encryption, hash algorithms

Cyber Operations

- Hands-on opportunity to conduct cyber operations in lab
  - Network reconnaissance, attack, defense
  - Digital forensics

Components of the Cyber Domain

What makes up the “Cyber Domain” anyway?

- Are there aspects other than just computers?
- What about systems connected to computers?
- Is the physical location of the system of interest?
- Are we a part of the cyber domain?

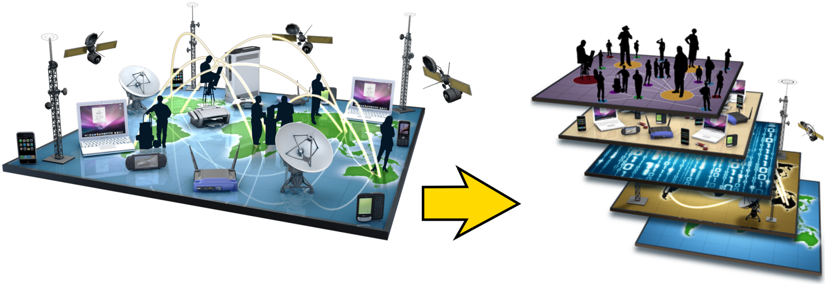
Not just computers

Many aspects of the cyber domain:

- Human Factors
- Information Technology
- Physical Systems
- Geography

Aspect Model

Breaking down the Cyber Domain.



Persona Aspects

What is it?

- Users that are taking part in the Cyber Domain
  - Using information systems, networks
  - Motivations and roles:
    - Nefarious/malicious
    - Beneficial
    - None

Interface Aspects

What is it?

- Hardware devices and software that users use
- How we interact with the Cyber Domain
  - Keyboards and mice
  - Touchscreens, cameras, microphones

Logic Aspects

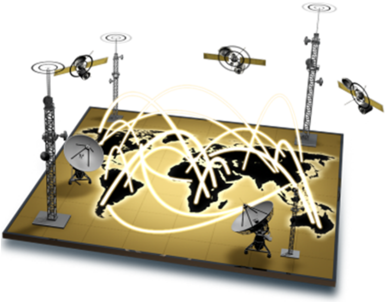
What is it?

- Information stored on and being transferred between information systems

Circuit Aspects

What is it?

- Paths on which data flow between systems
  - Ethernet cables, WiFi
  - RF transmission links
  - Fiber-optic cables
  - Satellite links



Geographic Aspects

What is it?

- The physical location of the user, system, or data path
  - Includes natural boundaries (mountain ranges, oceans, lakes) and geopolitical boundaries (separating countries, etc).
  - Why might this be important?
  - Example: Baltimore tunnel fire

The Reality

- Cyberspace is Technology + People + Processes
- Wealth and Treasure is Stored There 24/7
- Virtually Every Other Domain Depends on It
- Threats are Significant, Agile, and Growing
- Security is Impossible; Defense is Possible

Questions

Questions?

Saved rounds

- Read Lecture: Intro to Cyber Domain
- Finish HW (Due at start of next meeting!)
- Be on the lookout for a software installation email in the near future