Class/Article Notes:

Cyberwar (Amy Zegart):

* Cyber-attack from the poorest country on earth started a national security discussion/incident
* Cold war: knew adversary location, motives, capabilities
* Today’s threat?
* 2009 Cyber Threats were not recognized
* 2015 – cyber threats are at the top of the threats list
* Possibilities:
  + Degrade military
* Cyber is Different:
  + Most powerful = most vulnerable
  + The government cannot go it alone
    - 85% of critical infrastructure is owned/operated by private entities
  + The Attack surface is huge (no safe neighborhoods): good guys/bad guys always connected
  + Victims don’t know they are victims
    - Worm – infected gov PCs for 14 months prior to detection
  + Short warning period before attack; long time required for response (attribution)
* More than 40% of the world is on the Internet
* Growing IoT world (always vulnerable)
* 1 defect for 2500 lines of code
* Android phone: 5000 vulnerabilities
* Windows: 25 mil lines of code
* Cyber Threats of today: annoying
* Cyber Threats of tomorrow: cars, planes, power, water, weapons, (everything that

Question: Are we the most connected government/country? What about those that are more digitized (Krimea?)

Governments Don’t Understand Cyber Warfare. We Need Hackers (Rodrigo Bijou):

* We have an opportunity to make millions of people safer all over the world. Will we take the opportunity?
* Governments are too slow, we need to give up power and control to others (this sounds like The Avengers hacker style)

Definition of Cyber and Cyberspace:

Joint Publication 3-12:

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

JP 3-12 discussed the three interrelated layers of cyberspace which include the physical network, the logical network, and the cyber-persona.

JP 3-12 does not define “cyber” as a stand-alone term, however it is used frequently throughout the documents, most notably as the C in USCC (United States Cyber Command). Therefore, the U.S. now has a Combatant Command with a title that we can’t even define. (No wonder we have a hard time talking about this topic)

Each time the term “cyber” is used it seem so be a discriminator, meaning that it distinguishes it from related terms in other domains or arenas. This can be seen in the term “cyberspace” which is defining the space in which cyber activities take place differentiating them from land, sea, air, and outer space.

Therefore, I would define cyberspace similar to JP 3-12 but add several important features of cyberspace including that it is created and manipulated by humans and that it includes those systems that are “stand-alone” in nature.

My definition: Cyberspace is a domain created and manipulated by people consisting of the interdependent and stand-alone networks of information (data) and information technology.

Now that we have a solid definition of cyberspace, we can move to the idea of cyber. This seems backwards, but I think it is important to define the arena where “cyber” takes place in order to actually define the activity itself (IF cyber is only an activity).

My definition: Cyber is an adjective or adverb that refers to conflict between actors (human or machine) occurring in or through cyberspace.

If I am understanding your point about conflict being inherent in cyber, I disagree on the basis that actors (or “cyber-personas” as defined in JP 3-12) manipulate or change cyberspace without the thought of conflict entering their minds. Activities as harmless as posting on Facebook, setting up a new home computer, or connecting two supercomputers to conduct academic research are not part of conflict. However, these activities are happening in and through cyberspace and are changing the cyberspace domain. I would call these cyber activities. This means that much of what is called cyber today does deal with conflict in the digital world, however it does not include everything that could be, and I think should be, included in the term cyber and its domain cyberspace.

Thanks for a great discussion. I am looking forward to Wednesday’s class.

Research Paper Topic: I am planning to focus my research on cyber workforce development and training. Specifically, I will highlight the effectiveness of gamification and social interaction in the support of education for both cyber professionals and those without a direct link to cybersecurity. As part of the research, I will explore how the Air Force is training its cyberspace operations officers that do not currently work in a cyber operations organization. Since this paper will focus on broad areas of cyber workforce development, I am planning to submit it to the European Conference on Cyber Warfare and Security. Additionally, since there is a strong Air Force connection I will also try to submit it to the Armed Forces Communications and Electronics Association (AFCEA) Cyberspace Symposium in Colorado Springs, CO in February 2019.

Video Topic: I currently have two ideas for my video and would prefer to do the first option if the timetable is suitable for the class.

1. Present my research paper. Since my research will be connected to a solution such as the Cyber Education Hub, I would like to make a video the shows and explains the different features of the CEH and how DoD cyber professionals can use and contribute to the CEH. The video will specifically target Cyberspace Operations Officers who are outside of operational cyber billets and may not have the resources at hand to keep up with the fast pace of cyber.
2. If the first video idea has already been accomplished, or will not be achievable during this course, I will create a video discussing practical methods for Two Factor Authentication and password security. These are solutions that could be relevant to AF members, but also anyone who uses a password or authentication site. Easily cracked passwords, duplicate passwords, and lack of multi-factor authentication still pose significant threats in cyberspace. In 2018 alone Verizon reported that there were 38,000 successful attacks using botnets to target individuals in order to steal their credentials and use them on banking applications and other sites requiring authentication. These credentials are also being used to successful access corporate networks due to duplicate credentials for multiple systems.[[1]](#footnote-1)

Cyber Tactical:

* TTPs
* Surveillance
* Recon
* SCAR
* Strike
* Access

Cyber Operational:

* Uncertainty
* Espionage
* Disrupt/Degrade/Deny/Destroy/Detect
* Deceive
* Distract

Cyber Strategic

* Deterrence
* Influence
* Discredit
* Doctrine/Policy
* Cyber-Physical Attack
* Stealing Tech
* ISR

Multi-Domain C2:

* Jam comms in Land/Air
* Disrupt adversary C2 prior to land/air/sea attack
* Disable assets
* Take control of adversary assets
* CAS (land/air)
* Prep battlespace by softening
* Dumping fuel
* Mis-Info: logistics, battleplans,
* It is about creating effects, not using capabilities
* We need warfighters first and then (maybe) have a specialty

Army: Mission to Task; Order to Purpose

Notes on “21st Century Hackers” - <https://www.youtube.com/watch?v=koi54cPRlhQ>

* Shows a laymans overview of modern-day hackers, but quickly becomes focused on privacy concerns. They promote TOR (The Onion Router), as a solution to use technology while protecting privacy.
* The comment that protecting privacy as a human right is the same as protecting liberty is true. This fact is supported by the

How/when to employ a cyber weapon?

* Unrealistic expectations
* Ambiguity hinders us in defining the problem and coming to viable solutions
* Increase cyber arms race when weapons are deployed
* Leadership doesn’t understand capes
* How does our historical context?

Cyber Warrior:

* Abstract Thinking
* Comfortable w/ rapid tech change
* Continuous Learning
* Agile & Adaptable
* Critical Thinking
* Technical Expertise
* Profession of Arms:
* Ethics
* Communication

ACC/A6 Conference:

* ITaaS – this is going to happen.
  + What about questions over contracts, services, visibility?
  + What happens when there is a breach? Do we assign fault? Do we take money from the contractor?
* Who is doing records management? COMSEC? Support functions?
* How do we fulfill congressional mandates?
* How do we get from where we are today (encumbered by support) to the sexy cyber stuff?
* Make sure our community understands the warfighting language and warfighting effort.
* Write requirements to capture impact. Example: “Need capability to deliver warfighting capabilities/training/etc. to those that need it.”
* Need to become a software development company
* Need multi-domain capabilities to neutralize threats and push us back into “great power conflict”
* Need to have users at the center of app development
* Gen Weggeman (ACC/VC): multiple paths to greatness in the the cyber career field
* Human Performance – how much can a human take in and take action on?
  + Information is moving so quickly and accumulating quickly, how can we keep a human in the loop, but reduce

Cyber Weapons:

* AFINC – Boundary Defense and visibility (blocks 80% of attacks)
* CDA – Watching for spillage; BDA
* ACD – investigations; AFCERT, what happened and how did it happen; need to either watch or remediate; enterprise DCO
* CSCS – Operation and Maintenance; provide core services. Blocks attacks that get past the GW,
* CVA-H – Cyberspace Vulnerability Assessment – Hunter; Used by CPTs and MDTs
* C3MS – Cyber C2 Mission System; C2;

Why Designate Cyber WS?

* Tooth & Tail (big teeth requires big tail)
* Capabilities

Capabilities and Military Operations:

* HBSS is just a Sensor Net (this puts it into military language)
* Make our data actionable
* We can’t expect our leaders to learn more about technology
* Military Operator First and cyber geek second

Cyber and Contract Requirements:

* Need to apply creativity but guard against something that is not plausible or true

Cyberspace Deterrence:

* Passive & Active
* Tit-for-tat
* Attribution is complicated
* May want to de-escalate (off-ramps)
* Are cross-domain actions are appropriate?
* Proportionality can be tricky because of 2nd & 3rd order effects
* Need better guidelines
* Need to strike fear in attacking us
* Cyber arms race is part of that
* Need diversity in strategy

Anatomy of Attack:

* Recon
* Scan and Enumerate
* Find vuls & exploits
* Establish a foothold
* Elevate Privileges
* Create Backdoors
* Eliminate Evidence

Strategic Strengths:

* Diversity
* Sophistication
* Mass/Maneuver
* Defense Industrial Base
* R & D
* Cyber Patriot
* Cyber militia
* Weave Cyber Capes into DIME
* Can we run out of cyber capabilities?
* National Infrastructure (high speed internet)
* Vuln Patch (public awareness of vulnerabilities)

Triangles of Design:

1. Security, Usability, Functionality
2. Vulnerability, Exploit, Threat

1. "2018 Data Breach Investigations Report." Verizon Enterprise Solutions, accessed October 10, 2018, 4. https://www.verizonenterprise.com/verizon-insights-lab/dbir/. [↑](#footnote-ref-1)