My name is Michael Lanham and I split my time at West Point between teaching and the Cyber Research Center.
I will provide a brief overview of West Point, before discussing the specific points our hosts asked me to address.
Mission: To **educate, train** and **inspire** the Corps of Cadets so that each graduate is a **commissioned leader of character** committed to the values of Duty, Honor, Country and prepared for a career of professional excellence and service to the nation as an officer in the United States Army.

- 47 months
- Three programs for assessment:
  - Academic
  - Military
  - Physical
- ~4,400 cadets
- Graduate ~1,000 per year

West Point’s Mission is to Educate, Train, and Inspire leaders of character. It is a 47 month college and military experience evaluated in three areas. I briefly discuss the academic program and how the cyber domain is impacting it.
• Graduates anticipate and respond effectively to the uncertainties of a changing technological, social, political, and economic world. (emphasis added)
  – IT Goal: Graduates understand and apply information technology concepts to acquire, manage, communicate, and defend information, solve problems, and adapt to technological change. (emphasis added)
  – 8 other goals to include developing moral awareness, understanding human behavior, and cultural perspective(s) (emphasis added)

The Academic program’s overall goal is this first bullet, and I’ve added emphasis to the concepts we are discussing here in this seminar.

The overall goal has 9 sub-goals, and I show the Cyber-specific goal here.

I also included a few key phrases from the other 8 sub-goals, as a point of emphasis that West Point is very aware of the human element of educating and training officers.
This slide depicts West Point’s curriculum in cyber topics from a high level. I’m happy to discuss the many parts of this slide during breaks, but the main point is that West Point has made a deliberate effort to incorporate technical and non-technical discussions of cyber in many parts of our curriculum. The expectation is building confidence via repetition and exposure

----------for one-on-one discussions-----------------------------------

For every cadet, it begins with IT105 in the first year. In their second year students pick their respective majors.

The majority select non-technology majors. On this branch, cadets touch on Cyber at several points in the core curriculum. IT305, Theory and Practice of Military Information Systems, is the required for all of these students. Nine electives in three departments are available on cyber topics: cryptography, game theory, national security law, are a few examples.

A smaller group selects a major where cyber can be studied in depth. It’s a rich program featuring hands-on exercises and a system design-build-test experience in the senior year. Additionally, we offer various extracurricular activities.

We offer about 50 summer internships per year related to cyber. These are available to all cadets.

The total West Point program earned certification as an COE in 2002. We were the first undergraduate program to be so-designated.

The majority of these courses are taught by 10-15 year in Service Captains, Majors, and Lieutenant Colonels who return to the field force with exceptional knowledge and leader competencies.
Beyond teaching confidence with tools, West Point constantly emphasizes that the core of our Army is our Soldiers—not their particular types of helicopters, tanks, rifles, or computers. This does not change in the face of cyber events, as it does not change in the face of rifle or artillery fire.

However, we also teach that the Army operates as part of a whole, and within that whole there is history to learn, old and new trends to incorporate, and they need to stay aware of the political and legal landscapes. Cyber education is not simply about buffer overflows and firewalls, attack and counter-attack.

- The Army’s mission is to fight and win the Nation’s wars...
  (http://www.army.mil/info/organization/)
  - In the end, it is not the quality of weapons, but the quality of Soldiers employing them that determines mission success.” (Army Doctrine Pub 1, 2012) (emphasis added)
  - No change under cyber threats or cyber attacks!

- Common non-technical cyber information & themes
  - History of cyber events & cyber-focused commands
  - International and national law questions & research
  - Classification of events—pranks, crime, espionage, force
  - Policy development, analysis, and selection

Cyber is integrated with military education
West Point remains focused on generating officers to lead small units. One of the key tasks for small unit leaders is to conduct rehearsals and training for immediate action drills. A topic of conversation includes when and how to incorporate cyber rehearsals into training—when can it become a training distracter versus a training objective.

The Army is also borrowing an old technique—we have begun to commission technical specialists directly into technical units.

West Point does not teach high-ranking officers, though that topic may be an excellent follow-up for this seminar.
As teachers, we’ve all helped students survive the degraded cyber environment – usually by not accepting ‘my hard drive died last night’ as the newest reason for missing deadlines.

In military training, West Point helps cadets learn manual soldier skills long before we integrate cyber capabilities. By learning to perform to standard without the aid of advanced capabilities, cadets know they can adapt if they need to—even as they acknowledge the advantages that IT brings to the Army.
• Leaders
  • Able to operate with imperfect information
  • Able to control ‘information addiction’—withdrawals & unsatisfied expectations are rarely pretty
  • Rehearse realistic degraded-cyber battle drills
    – Short term (akin to night time training, casualty training, fire drills)
    – Sustained periods & varying degree (enough to overcome the ‘just wait it out’ reaction to typical network outages)

Operating with imperfect information is a skill West Point constantly reinforces with cadets. We also reiterate in multiple forums that information addiction is a disease that affects all echelons—control what they demand from subordinates.

Returning to small unit leader tasks....rehearsals of tasks breed competence and confidence. Competence and confidence establish resilience to degraded cyber environments!
Along with cultivating individual officers, West Point tries to teach officers how to create appropriate command climates suitable to chaotic environments.

To cope with the chaos of warfare, the Army has, for a very long time, tried to teach its commanders to give orders about ‘what’ and ‘why’ but without specifying ‘how’ to accomplish the task(s). This effort and its evolutionary descendant is called ‘mission command’ and has 6 key principles. Trust (up and down the chain of command), initiative by subordinates when coping with unexpected situations, continuation of ‘what’ and ‘why’ without the specified ‘how.’ The last principle is the fundamental acceptance that risk is unavoidable, but should be accepted in prudent circumstances, not simply for the sake of risk acceptance.

The last point about command climate is that it is fundamental to ensuring Soldiers adhere to Rules of Engagement, and the public laws that shape those ROE.
Questions
Backup Slides
West Point builds confidence with cyber through repetition and broad exposure

Non-technology majors take one of several 3 course engineering sequences

Anyone with room in their schedule and interest can take the new Cyber Minor

We offer a variety of cyber elective beyond traditional CS or IT classes

We offer the CDX to majors and the competitive cyber capture the flag team is open to all with skill
• Inspiring Cadets
  – Three week cyber internships
  – Voluntary (consumes leave time)
  – 2014 Opportunities
    • Google
    • Disney information Security
    • FireEye
    • US Cyber Command
    • United States Secret Service
    • Army Cyber Command
    • National Cyber-Forensics and Training Alliance (NCFTA)
    • Looking Glass Cyber Solutions

Inspire through exposure to breadth of ‘cyber’
• Service trains, mans and equips the total force for all warfare—cyber competes with many other interests

• Requirements and capabilities analysis with formal framework
  • **Doctrines** Organization
  • **Training** Material Solution
  • **Leadership** Personnel
  • **Facilities** (DOTMLPF)

• Examples of **bold** framework components include
  • Integration within existing C2 structures and organizations
  • Integration with Joint Commands, National Guard, Reserves
  • Initial and recurring training for all ranks
  • Career progression for all ranks
  • Integrate with traditional military functions (offense, defense, stability operations, and homeland defense)

---

**Be flexible... Cyber is more than IT, just as Army is more than Infantry**
Army Organizing / Providing Capability

Army Cyber Command
Cyber Operations

Cyber Support Team
Cyber Support Team
Cyber Support Team
Cyber Support Team
Cyber Support Team
Cyber Support Team

Army Cyber Center of Excellence
(Army Training Center)
Cyber Propaganda
LOJIMPLF

Army Cyber Institute
Outreach
Advisory
Research - Educate

Army using multiple organizations to design and implement cyber