Deterrence and Power: Military use of cyberspace

Dr. Heather A. Harrison Dinniss
International Law Centre, Swedish Defence University
Outline

• How do States and armed forces think about cyber?
• What is the role of the armed forces?
• What options do we have?
How do Armed Forces (generally) think about cyber?

- Cyber as a domain of operations
- Capability and Capacity Planning
  - Strategies
  - Thresholds
  - Reconnaissance & Mapping

Legal issues

- Integrated and stand-alone operations
What is the Role of the Armed Forces?

• Primarily responsibility for security the armed forces networks!
• Role depends on who is attacking - Attribution issue
• May be asked to support the police, pt with regard to terrorist crimes
• Responsibility for defence if an armed attack occurs
Deterrence

• What is deterrence?
  • The ability to alter an adversaries actions by adjusting its cost-benefit calculations.
  • ‘deterrence is the threat to use military force to impose intolerable costs if an opponent takes an unacceptable action’.

• Can/does cyber deterrence work?
  • Preferred responses are covert
  • Viewing deterrence from a purely military perspective is unworkable for cyber
  • Viewed more broadly, ... perhaps...!
Other Options for Coercion?

• Indictments
• Name and shame
• Countermeasures
• Offensive Cyber Operations