

Overview of the course “Information Security and Cyber Warfare”

Goals (from the syllabus)

- Understand the theory and practice of cyber power and cyber warfare
- Understand fundamental concepts of computer and network security, cryptography, and software vulnerabilities
- Improve skills for writing about issues that involve both technology and policy considerations
- Gain rudimentary practical experience of performing and defending against security exploits

Non-goals

- Become an expert hacker
- Learn how to program
- Become a certified information security professional

Design of the course

- The course is designed so that anyone can succeed in the course, regardless of background knowledge
 - No computer science or programming knowledge is assumed
- Course content is 50% geopolitical, 50% technical
- The geopolitical material is based on readings from the required texts
 - Qualitatively similar to the introductory International Relations course
- The technical material is based mostly on lectures with some readings for background information
 - Qualitatively similar to a first-year seminar on a science topic
 - Includes four practical lab sessions in which students work in pairs, experimenting with some simple computer programs

Main topics

Technical content

Geopolitical content

- password security
- cyber war overview
- cryptography
- cyber power of states and terrorist organizations
- software vulnerabilities
- cyber warfare in more detail
- computer security
- other, e.g. cyber crime, international law issues