Course ID

CYBERSEC

Course Duration

2 days

Course Type

Private Class

Course Title

Cyber Security and Cyber Warfare

Related Courses

- Policy of Cyber Space and Cyber Conflict (CYBERPOL, 2 days)

Aimed At

Information/communications industry professionals, business or government security professionals, and others interested in learning how the changing landscape of cyber security impacts telecommunications technologies.

Group Size

5-25

Prerequisites

General familiarity with telecommunications.

Course in a Nutshell

A spate of cyber-attacks, some of which were quite persistent and severe, have recently affected government agencies as well as businesses in a wide range of industries, including the CIA, US Senate, IMF, Google, Lockheed Martin, Sony, Citigroup, and others. This has led the Pentagon to enunciate a formal cyber strategy and Leon Panetta, the US Defense Secretary, to warn that “the next Pearl Harbor we confront could very well be a cyber-attack.”

This two day course addresses the key issues of cyber security and cyber warfare. We will begin with an introduction to information, network, and computer security. We will then discuss in detail how these technologies can be influenced and attacked at a national, strategic level as part of a cyber-warfare campaign. The course is taught by someone currently involved in pushing the state-of-the-art of cyber security/warfare and is continually updated to include the latest research.

Customize It!

We can customize the content and duration of this course to the needs of diverse participant groups in business or government (military, homeland security, intelligence community). We can also calibrate the course’s “tech level” to the nature of the audience, such as technical professionals, managers/executives, or policy makers/strategists.

Learn How To

- Describe the basics of information, network, and computer security
- Describe how cyber security impacts military strategy for cyber warfare

Course Outline

- Introduction to Cybersecurity
  - Information Security Fundamentals
    - Confidentiality, Integrity, Availability
    - Disclosure, Deception, Disruption, Usurpation
    - Security Policies vs. Mechanisms
    - Trust and Assurance
  - Cyber Systems and Security
    - Systems and Networks; Hardware and Software
    - Protocol vs. Platform Attacks
    - Attack and Exploitation Tools
    - Defensive Tools
- Critical Infrastructure and Key Resources (CIKR)
- Industrial Control Systems
  - Supervisory Control and Data Acquisition (SCADA) Systems
  - Security of Embedded Control Systems
  - Case Studies in Power, Stuxnet
- Business as Critical Infrastructure
  - Financial Institutions
  - Intellectual Property Theft
- Internet Robustness and Survivability
  - BGP Routing Infrastructure
  - Economic and Political Aspects of Internet Governance
  - Internet Availability and the World Economy
- Impact and Risk of New Technologies
  - Smartgrid
  - Intelligent Transportation
  - Cloud Computing
- Military Aspects of Cyber
  - Cyber as a Warfare Domain
  - Cyber as a Weapon System
  - Cyber Kill Chain
  - Net-Centric Warfare
- Impact of Cyber on Military Operations
  - Command and Control
  - Mission Planning and Execution
  - Impact of Availability on Mission Success
- Cyber Strategy and Tactics
  - Computer Network Operations
    - Computer Network Defense
    - Computer Network Exploitation
    - Computer Network Attack

  - Electronic Warfare and Information Operations:
    - Electronic Attack
    - Electronic Protection
    - Electronic Support
  - Case Studies: US and India

- Military Cyber Doctrine
  - Rules of Engagement
  - Proportional Response
  - Collateral Damage
  - Impact on Foreign Policy
- Case Studies: China and Google; Russia and Georgia; Estonia
- Wrap-up
  - Course Recap and Q/A
  - Evaluations

How You Will Learn

- A researcher who is at the forefront of cyber security/warfare will present this course in interactive lecture format.
- Along with the lecture, we will use discussion and group activities to enrich the classroom environment and convey the important points.
- We will compare and contrast what's already familiar to you with what's new, making the new ideas easier to learn as well as more relevant.
- If your background is less technical, we will use meaningful and ingenious examples and analogies to simplify the complex subject matter.
- You will receive a printed Participant Handbook which will help you remember and retain what you learned in class and apply it on your job.

Revised *July 21, 2011f*