Study Guide
College of Information Security & Assurance
ISA 450
Modern Cyber Conflicts

Description

1. Take an event or development in cyber-conflict and perform an historical case study;

2. Questions will test students knowledge of concepts introduced via class, book, and online discussion.

Exam Requirements

Blue Book format.
Paper and Pen.
1 hour test.

Evaluation Criteria

Submissions will be evaluated based on originality, strength of argument and recommendations, adherence to the norms of spelling, grammar, and syntax, and clarity.

Originality: Has the author identified and defined the central issue? Is this issue of major importance to the intelligence community or of major concern to users of intelligence? Has the author revisited a known issue and proposed a new approach or solution, or has the author defined an issue or approach from a new perspective?   **Weight: 35 Points**

Research and Analysis: Has the author done original research, such as interviews or use of primary material, to bolster their paper? Are the facts and opinions from this research analyzed to make a coherent case on how and why this incident is historically relevant? **Weight: 35 Points**

Clarity: Is the author's product clearly presented and well organized? Is the issue clearly described and documented with the recommendations and proposed outcomes precisely laid out? Is the writing clear and lucid? **Weight: 20 Points**

Spelling, Grammar, and Syntax: Has the author prepared a grammatically correct and properly edited entry? **Weight: 10 Points**

Case Studies for Exam

Case Studies
One of the following Case studies will be on the exam:

- Cuckoo's Egg (~1986)
- Morris Worm (1988)
- ELIGIBLE RECEIVER (1997)
- SOLAR SUNRISE (1998)
- MOONLIGHT MAZE (1999)
- Cyber conflict in Georgia (2008)
- Operation Buckshot Yankee (2008)

Exam Type Questions
Four questions, a combinations of questions, or variation of similarly liked questions will be on the final exam:

- What is Cyber Warfare?

- What is the United States Doing About the Threat of a Cyber War?

- Have We Seen a Cyber War?

- What do we mean by battlespace?

- Where does Cyber Fit in the War-fighting Domain?

- What is threatscape?

- What are the challenges for fielding systems at the speed of need?

- What are the three functions under CNO. Explain in detail the purpose of each.

- Discuss U.S. Doctrine and purpose of INFOCON.

- What does a Cyber Warrior look like?

- How are the physical and logical realms connected? What types of tools can an adversary use to conduct Cyber Conflict?

- How does the military approach social engineering? Discuss the different progressional phases. Provide examples of how HUMINT can lead to the extraction of information.

- Discuss the differences between reconnaissance, survelliance, and APT. How can HUMNIT and OSINT be used to conduct activities. How do the three functions of CNO relate.

- How does Cyber warfare capabilities change the way conventional warfare is carried out? Cite examples of Proactive vs Reactive.

- Describe the attack process

- In computer Network Defense the goal is to protect security objectives such as Confidentiality, Integrity, and Availability. Describe the difference for each and provide examples. What is the most important security objective for the U.S. military? Is it more important to protect the system or the information?

- Does defense in depth work? Why or Why not?

- Should the U.S. government be using "the carrot or the stick" to motivate industry? For example, should the government be provide rewards for proactive cyber defense or rule with regulations and penalties?