Appendix B

Syllabus of Qualifying Examinations

PhD in Engineering with a focus in Security

Computer Communications
Fundamentals of Computer/Network Security
Applied Cryptography for Secure Communication
Homeland Security and Defense

Computer Communications
Syllabus of Qualifying Examination
PhD in Engineering with a focus in Security
Reference course: CS5220 Computer Communications, College of EAS, UCCS

Created by Prof. Xiaobo Zhou and Prof. Edward Chow, last updated February 2008

Description:
Communication networking is one of the most exciting and important technological fields of our time. The Internet and its applications and services are changing the ways we live and work. The computer networking field and all that it enables is a vast new frontier, full of amazing challenges. There is always room for innovation.

This examination covers fundamental computer networking concepts and principles. People should be able apply the networking theory and design principles, verify their understandings, and build a solid foundation for creating innovations in today's Internet. The reference course lays foundations of network architectures, protocol design principles, and TCP/IP programming skills, which are necessary to take more advanced courses in graduate study and/or technical training in the industry. It also covers basic networking knowledge, network configuration and programming experience, and in-depth understanding of the inner-workings of computer networks and their evolution. Communication systems, from simple to asynchronous point-to-point links, to those based on complex network architectures will be examined. Material will be oriented toward the computer scientist as a user, designer and evaluator of such systems.

Reference Textbooks

Highly Recommended: Alberto Leon-Garcia and Indra Widjaja, "Communication Networks", 2nd Edition, McGraw Hill, ISBN 0-07-246352-X.

Alternatives:

Andrew Tanenbaum, “Computer Networks”, 4th edition, Prentice Hall, ISBN 0-13-066102-3

Larry Peterson and Bruce Davie, “Computer Networks”, 4th edition, Morgan Kaufmann, IBNS 0-12-370548-7

Covered Topics

- Evolution of Network Architecture and Services
- The OSI Layered Model
- Socket Programming
- Digital Transmission Fundamentals
- Error Detection and Correction
- Multiplexing
- ARQ Protocols and Reliable Data Transfer Service
- Sliding-Window Flow Control and TCP Reliable Stream Service

- Data Link Controls
- Medium Access Control based on Random Access
- Medium Access Control based on Scheduling
- Performance Analysis of Medium Access Control Protocols
- Ethernet and IEEE 802.3 LAN Standard
- Wireless LANs and IEEE 802.11 LAN standard
- LAN Bridges and Ethernet Switches
- Datagrams and Virtual Circuits
- Routing in Packet-Switching Networks
- Shortest-Path Routing
- Traffic Management at the Packet Level (Fair Queuing and Priority Queues)
- Traffic Management at the Flow Level (Congestion Control)
- The Internet Protocol (Subnet and CIDR)
- TCP/UDP Protocols
- Internet Routing Protocols (RIP, OSPF, BGP)
- Multicast Routing
- NAT and Mobile IP
- Integrated Services
- Differentiation Services
- Quality-of-Service Provisioning
- Multiprotocol Label Switching (MPLS)
- Real-time Transport Protocol

Background Expected

- Computer Architecture and Operating Systems
- C/C++ and/or Java Programming

Fundamentals of Computer/Network Security
Syllabus of Qualifying Examination
PhD in Engineering with a focus in Security
Reference course: CS5910 Fundamentals of Computer/Network Security, College of EAS, UCCS

Created by Prof. Edward Chow, last updated February 2008

Description:
Computer and network security is critical to the operation of today's information systems ranging from the national cyber infrastructure, IT systems of companies, and individual home computers. With constantly evolving cyber attacks and defenses, this is an exciting, important, and challenging area for research.

This examination covers fundamentals of computer and network security. Students will be tested on their understanding of the basic cyber attack and defense techniques and should be able apply the design principles for security mechanism to analyze the vulnerabilities of a network system, to examine the risk of security in computing, and to propose a secure solution. Given a piece of code with potential security holes, students need to be able to identify them and suggest patches or solutions to seal off the security holes. Given the internet traffic patterns and service requirements, students need to be able to configure a secure network with the firewall and IDS components to filter out the malicious code and block illegitimate access patterns.

Reference Textbooks

- Ross Anderson, "Security Engineering," 2nd Edition, John Wiley & Sons, ISBN 0-471-38922-6, 2008. He also put this book free online. http://www.cl.cam.ac.uk/~rja14/book.html.
- Chapter 8 of Andrew Tanenbaum, "Computer Networks", 4th edition, Prentice Hall, ISBN 0-13-066102-3

Alternatives:

- Charles P. Pfleeger, Shari Lawrence Pfleeger, "Security in Computing," Prentice Hall, ISBN: 0-13-035548-8, 2003.
- Matt Bishop, "Computer Security: Art and Science" Addison Wesley Professional, ISBN 0-201-44099-7, 2003.
- William Stallings. "Network Security Essentials: Applications and Standards," 3rd Edition, Prentice Hall**, ISBN-13:** 978-0132380331, 2006.
- Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public World", 2nd Edition, Prentice Hall, ISBN-13: 9780130460196, 2003.

Covered Topics

- Design Principles for Security Mechanism, Basic Security Services.
- Penetration Testing: NMap, Nessus, Metasploit Framework.
- Malicious Code: Virus, Worm, Trojan, Slammer.

- Buffer Overflow and its defenses.
- Firewall: Netfilter, iptables, DMZ
- Instruction Detection/Prevenetion Systems: HIDS, NIDS, snort, tripwire.
- Denial of Service (DoS), Distributed DoS, and their defense.
- Security Models, Multilevel Security, Trusted Solaris, SELinux

Background Expected

- Unix Systems
- C

Useful References:

- Glossary: Internet Security Glossary: rfc2828 by Bob Shirey of GTE/BBN May 2000. http://www.faqs.org/rfcs/rfc2828.html
- National Information Assurance (IA) Glossary by CNSS, revised May 2003. http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
- Buffer Overflow:
    - "Smashing The Stack For Fun And Profit," by Aleph One.
    - "On the Effectiveness of Address-Space Randomization," by Shacham et al at Stanford's applied crypto group at ACM Computer Communication Security Conference 2004.
- Malicious Code:
    - Slammed! An inside view of the worm that crashed the Internet in 15 minutes, by Paul Boutin, July 11 2003 Wire magazine. http://www.wired.com/wired/archive/11.07/slammer.html
    - The Spread of the Sapphire/Slammer Worm, by David Moore Vern Paxson Stefan Savage Colleen Shannon Stuart Staniford Nicholas Weaver. http://www.caida.org/publications/papers/2003/sapphire/sapphire.html
- Reflections on Trusting Trust, by Ken Thompson's 1983 Turing Award lecture. ACM Digital library.
- OS Hardening wiki. http://viva.uccs.edu/wiki/
- Cross Domain Solution wiki. http://viva.uccs.edu/cds/
- iCTF wiki. http://viva.uccs.edu/ictf/
- Secure Programming for Linux and Unix HOWTO, by David Wheeler. http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html
- Secure Web Access Web page. http://cs.uccs.edu/~cs591/secureWebAccess/secureWebAccessNew2.html
- Firewalls:
    - iptables tutorial 1.2.2 byOskar Andreasson. http://iptables-tutorial.frozentux.net/iptables-tutorial.html
- IDS:
    - Snort Users Manual http://www.snort.org/docs/snort_htmanuals/htmanual_280/
    - minimal installation guide
    - NIST IDS Survey document, by Rebecca Bace and Peter Mell http://cs.uccs.edu/~cs591/ids/NISTsp800-31.pdf

    - Anomalous Payload-based Worm Detection and Signature Generation, by Wang et al, Raid 2005. http://cs.uccs.edu/~cs591/ids/raid2005Wang.pdf
    - HIDS: Tripwire, Implementing Tripwire. http://sourceforge.net/docman/display_doc.php?docid=2078&group_id=3130
- Penetration testing, *By Stephen Northcutt, Jerry Shenk,Dave Shackleford, Tim Rosenberg, Raul Siles, and Steve Mancini*. http://cs.uccs.edu/~cs591/penetrateTest/sanPortalWhitePaperPT.pdf
    - Metasploit framework. http://framework.metasploit.com/
    - OSSTMM 2.2. Open-Source Security Testing Methodology Manual, created by Pete Herzog. http://cs.uccs.edu/~cs591/penetrateTest/osstmm.en.2.2.pdf
    - Introduction to Nessus, scanning, analyze reports. http://www.nessus.org/nessus/ http://www.securityfocus.com/infocus/1741
    - Information System Security Assessment Framework (ISSAF Draft 0.1) http://cs.uccs.edu/~cs591/penetrateTest/issaf0.1.pdf
- Security Models, Multilevel Security. Bell-LaPadula model.
    - http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html
    - Chapter 3 Tour of Trusted Solaris Environment page 49 of trusted solaris user guide. http://cs.uccs.edu/~cs591/securityPolicy/trustedSolaris/trustedSolarisUserGuide.pdf
    - SELinux. http://fedoraproject.org/wiki/SELinux
- http://cs.uccs.edu/~cs591/homework.html
- http://cs.uccs.edu/~cs591/exam.html

Applied Cryptography for Secure Communication
Syllabus of Qualifying Examination

PhD in Engineering with a focus in Security

Reference course: CS5920 *Applied Cryptography for Secure Communication*, College of EAS, UCCS

Created by Prof. Chuan Yue, last updated June 2011

Description:

Basic security issues in computer communication, classical cryptographic algorithms, symmetric-key cryptography, public-key cryptography, hash functions, message authentication codes, digital signatures, key management and distribution, user authentication protocols.

This examination covers the basics of applied cryptography for secure communication. Students should know the fundamental security requirements, know the limitations of classical cryptographic algorithms, know the essential symmetric-key and public-key algorithms and their differences, know the basic requirements and mechanisms of message authentication, digital signature, and user authentication.

Reference Textbooks and Articles

- Cryptography and Network Security: Principles and Practice (5th Edition), by William Stallings, ISBN-10: 0136097049, ISBN-13: 978-0136097044

Covered Topics

- Overview of Security and Cryptography
- Classical Encryption Techniques
- Block Ciphers and the Data Encryption Standard
- Basic Concepts in Number Theory and Finite Fields
- Advanced Encryption Standard
- Block Cipher Operation
- Pseudorandom Number Generation and Stream Ciphers
- More Number Theory
- Public-Key Cryptography and RSA
- Other Public-Key Cryptosystems
- Cryptographic Hash Functions
- Message Authentication Codes
- Digital Signatures
- Key Management and Distribution
- User Authentication Protocols

Background Expected

- Integer arithmetic
- Modular arithmetic
- Algebraic structures

Homeland Security and Defense
Syllabus of Qualifying Examination
PhD in Engineering with a focus in Security
Reference course: PAD5950 Intro to Homeland Security and Defense, UCCS
Created by Center for Homeland Security (CHS), last updated February 2008

I. COURSE DESCRIPTION.

According to the *National Strategy for Homeland Security* (July 2002), "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur." Furthermore, according to *U.S. Northern Command's Strategic Vision* (September 11, 2003), U.S. Northern Command's mission is to "Conduct operations to deter, prevent and defeat threats and aggression aimed at the United States, its territories and interests within the assigned area of responsibility, and provide military assistance to civil authorities including consequence management operations as directed by the President or the Secretary of Defense."

This course provides an overview of homeland security, with an emphasis on homeland defense and U.S. Northern Command, its mission, the other government organizations it interfaces with, and constraints on those relationships. Course participants will gain an understanding of homeland security and homeland defense from the perspective of the primary national-level players: the Department of Defense, U.S. Northern Command, and the Department of Homeland Security. Military-civil relationships based on *Posse Comitatus* will be explored in depth.

Homeland security and homeland defense are new and evolving interdisciplinary fields. This course is designed to be an introductory graduate-level public administration course in homeland defense and will provide a foundation for follow-on homeland security and homeland defense courses.

II. EDUCATIONAL OUTCOMES/COURSE OBJECTIVES.

This course is designed to promote the educational outcomes expected of graduate students enrolled in the University of Colorado at Colorado Springs (UCCS) Certificate in Homeland Security Program and the Graduate School of Public Affairs (GSPA). Specifically, this course is designed to accomplish the following goals and objectives:

1. To increase your knowledge and understanding of the threat of terrorism and United States national strategies, policies, approaches, and practices to achieve homeland security and homeland defense.

2. To increase your knowledge and understanding of the role of the Department of Defense, North American Aerospace Defense Command (NORAD), and U.S. Northern Command (NORTHCOM) in homeland defense.

3. To address the legal, ethical, and privacy considerations of homeland security, national security, and defense issues.

4. To enable you to gain a conceptual and experiential grounding in the complex environment, multiple challenges, multifarious requirements, and interdependent processes faced by leaders, managers, and policy makers in establishing strategies and responses to counter terrorism and achieve homeland security and homeland defense.

5. To improve your ability to identify, describe, critically analyze, innovate, think strategically, and solve ill-defined homeland security and homeland defense problems.

6. To develop your skills for examining, discussing, and critiquing homeland security and homeland defense organizational roles, decision-making, and actions and the implications and consequences of homeland security and homeland defense activities.

7. To enhance your ability to listen and communicate accurately and precisely and to work effectively with others on homeland security and homeland defense issues.

8. To prepare you to be effective leaders and managers in homeland security and homeland defense organizations.

III. COURSE OVERVIEW.

The course emphasizes the following four major streams:

- The ***context and environment*** for United States homeland security and homeland defense.
- The ***nature and methods of terrorism*** and the ***challenges*** terrorism presents for homeland security and homeland defense.
- ***Issues, challenges, approaches, and solutions*** for homeland security and homeland defense.
- The role of the ***Department of Defense, NORAD, and U.S. Northern Command*** in homeland defense.

Readings from the primary textbook, government documents, and journals establish the foundation for course participant learning. Furthermore, case studies are used to augment and reinforce learning. The case studies provide course "experiences" of homeland defense activities and examples for analysis and discussion. The case studies selected are those that involve the above streams.

IV. REQUIRED TEXTBOOKS AND MATERIALS.

A. **Textbook.** The following textbook is required for the course. Course participants should obtain the textbook on their own and bring it to class on Week 2 (and other weeks) for discussion of assigned readings.

Cronin, Audrey Kurth and Ludes, James M., editors. *Attacking Terrorism: Elements of a Grand Strategy*. Washington, D.C.: Georgetown University Press, 2004.

B. **Case Studies.** The following case studies from the Kennedy School of Government (KSG) at Harvard University are <u>required</u> for the course. They are referred to as "KSG Case Study" in the

Schedule of Assignments. Course participants should review the case study abstracts available from the KSG Case Program through the web site at http://www.ksgcase.harvard.edu. Copies of the cases will be handed out in class prior to the session when they are required to be read.

1. #1709, "When Prevention Can Kill: Minnesota and the Smallpox Vaccine Program"

2. #1712, "Command Performance: County Firefighters Take Charge of the 9/11 Pentagon Emergency"

C. **Readings.** Required readings and sometimes additional or substitute readings will be (1) provided as handouts in class in advance of the associated class session or (2) posted on the "class page" on the NISSC web site in advance of the class session. Readings will consist of government documents, other public source documents, chapters from the textbook, articles from journals, and articles from newspapers or the popular press. For further enrichment, course participants are encouraged to read additional homeland security and homeland defense literature beyond the required readings. The instructor will occasionally distribute relevant articles from newspapers that provide extensive coverage of homeland security and homeland defense such as the *Washington Post*, *Washington Times*, *New York Times*, *Rocky Mountain News*, and *Colorado Springs Gazette* to generate class discussion of current issues. Course participants are encouraged to also share relevant articles with the class.

V. COURSE OUTLINE & EXPECTATIONS.

BLOCK 1 – THE CONTEXT, TERRORISM, AND COUNTERTERRORISM

Objectives

1. To know the course requirements, assignments, and outline of weekly sessions.
2. To understand the instructor's expectations of students for successful course completion.
3. To define "homeland," "homeland security," and "homeland defense."
4. To identify differences between homeland security and homeland defense.

Landmarks

1. There is a mutual obligation of the instructor and students to be respectful of others, prepared for class sessions, and professional in conduct.
2. Read the syllabus carefully to understand course expectations, requirements, and assignments.
3. Be ready for an important discussion of the differences between homeland security and homeland defense.

Discussion Questions

1. What is expected of students in terms of the reading assignments?
2. What is expected of students in terms of graded assignments consisting of the case studies, Homeland Defense Discovery Research Paper and In-Class Presentation, and discussion participation and attendance?
3. What are the definitions of "homeland," "homeland security," and "homeland defense"?
4. What are the differences, and implications of those differences, between homeland security and homeland defense?

Required Readings

Course syllabus.

Additional Recommended Readings
None

Lesson 1 - The Terrorism Threat to America

Objectives
1. To describe the nature and sources of terrorism.
2. To recognize the primary grievances terrorist groups have against the U.S.
3. To explain the intent, goals, and objectives of the U.S. *National Strategy for Combating Terrorism*.
4. To understand various strategy, grand strategy, and policy approaches for counterterrorism.
5. To discuss Constitutional constraints and the need for balancing both freedom and security.
6. To describe policy measures used by the executive branch to deal with terrorism.
7. To know the source and purpose of the "law of war".

Landmarks
1. Seek to truly comprehend the nature of terrorism in order to understand how to best counter terrorism.
2. It is essential to understand the U.S. national strategy of applying all elements of national power across four fronts to "defeat, deny, diminish, and defend" in order to achieve success in eliminating terrorism as a threat.
3. Creating an effective grand strategy is the major theme and thread that runs through the Cronin textbook. Get off to a good start with the Cronin textbook by paying close attention to this theme in the chapter readings assigned for this week.

Discussion Questions
1. How can understanding the foundation, nature, and sources of terrorism help in the global war against terrorism?
2. What will be required for an effective U.S. national strategy to counter terrorism?
3. What role does grand strategy play in a U.S. national strategy to counter terrorism?
4. Why did the founding fathers add the Bill of Rights to the Constitution?
5. Should a nation be willing to compromise on principles to achieve greater security?
6. Has the application of the Bill of Rights remained unchanged?
7. What's the inherent risk to waiving or curtailing civil rights?

Required Readings
Bruce Hoffman, "Rethinking Terrorism and Counterterrorism Since 9/11," *Studies in Conflict & Terrorism*, Vol. 25, Issue 5 (2002): 303-316.
National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Threat and Vulnerability" (pp. 7-10).
National Strategy for Combating Terrorism, The White House, February 2003. (30 pp.)
Department of State, *2003 Patterns of Global Terrorism*, 2004, "Overview of State-Sponsored Terrorism" (pp.1-9).
9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, Chapter 2, "The Foundations of the New Terrorism," (pp. 47-70).
Cronin and Ludes Textbook:
Audrey Kurth Cronin, "Introduction: Meeting and Managing the Threat," (pp. 1-16).

Audrey Kurth Cronin, Chapter 1, "Sources of Contemporary Terrorism," (pp. 19-45).
Martha Crenshaw, Chapter 3, "Terrorism, Strategies, and Grand Strategies," (pp. 74-93).

Additional Recommended Readings

New World Coming: American Security in the 21st Century, Major Themes and Implications, Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century, U.S. Commission on National Security/21st Century (Hart-Rudman Commission), September 15, 1999. (8 pp.)

Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom, Phase II Report on a U.S. National Security Strategy for the 21st Century, U.S. Commission on National Security/21st Century (Hart-Rudman Commission), April 15, 2000. (16 pp.)

Road Map for National Security: Imperative for Change, Phase III Report of the U.S. Commission on National Security/21st Century (Hart-Rudman Commission), February 15, 2001, "Preface" (pp. v-vii) and "Executive Summary" (pp. viii-xviii).

Fourth Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: IV. Implementing the National Strategy, December 15, 2002, "Executive Summary" (pp. iii-xi), "Chapter I. Introduction" (pp. 1-6), and "Chapter II. Reassessing the Threat" (pp. 7-26).

HSPD-2, *Combating Terrorism Through Immigration Policies*, October 29, 2001. (3 pp.)

HSPD-6, *Integration and Use of Screening Information*, September 16, 2003. (1 p.)

HSPD-11, *Comprehensive Terrorist-Related Screening Procedures*, August 27, 2004. (3 pp.)

Lesson 2 - Intelligence and Law Enforcement

Objectives

1. To know the separate roles, missions, identities, and cultures of the U.S. intelligence and law enforcement communities.
2. To understand the issues and challenges facing the U.S. intelligence and law enforcement communities in the war on terrorism.
3. To understand the need for and actions taken to improve relationships, increase coordination, and increase intelligence and information sharing between the intelligence and law enforcement communities.
4. To explain the scope, objectives, and actions of counterintelligence as part of *The National Counterintelligence Strategy of the United States* to help achieve national security.
5. To understand how the USA PATRIOT Act aids law enforcement efforts and arguments for how the Act helps achieve greater security and threatens civil liberties.

Landmarks

1. Reform and new approaches are necessary to get intelligence and law enforcement to work together in the war against terrorism.
2. Search for and read carefully references to the tensions between the intelligence and law enforcement communities and the tradeoffs between security and freedom.

Discussion Questions

1. Since 9-11, has adequate progress been made in improving how intelligence and law enforcement work together and is America safer from terrorism?
2. What are the major obstacles and what must be done to reform intelligence operations, collection, analysis, leadership, and organizations?

3. Why is the USA PATRIOT Act controversial and what is the future for its provisions?

Required Readings

Richard A. Best, Jr., *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, Congressional Research Service Report for Congress, CRS Report #RL30252, Updated December 3, 2001. (32 pp.)

National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Intelligence and Warning" (pp. 15-20) and "Domestic Counterterrorism" (pp. 25-28).

Office of the National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States*, March 2005. (13 pp.)

Office of the Director of National Intelligence, *The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, October 2005. (20 pp.)

Richard K. Betts, "Fixing Intelligence," (2002) Chapter 9 in *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, CT: McGraw-Hill/Dushkin, 2004). (pp. 459-469)

Alice Fisher, "The PATRIOT Act Has Helped Prevent Terrorist Attacks," Chapter 3 in *At Issue: Homeland Security* (Farmington Hills, MI: Greenhaven Press, 2004), pp. 34-42.

Nancy Chang, "The PATRIOT Act Has Undermined Civil Liberties," Chapter 4 in *At Issue: Homeland Security* (Farmington Hills, MI: Greenhaven Press, 2004), pp. 43-53.

Cronin and Ludes Textbook:

Lindsay Clutterbuck, Chapter 6, "Law Enforcement," (pp. 140-161).

Additional Recommended Readings

American Civil Liberties Union, "Homeland Security Measures Undermine Civil Liberties," Chapter 1 in *At Issue: Homeland Security* (Farmington Hills, MI: Greenhaven Press, 2004), pp. 13-22.

Stuart Taylor, Jr., "Homeland Security Measures Should Not Be Restricted by an Overly Broad View of Civil Liberties," Chapter 2 in *At Issue: Homeland Security* (Farmington Hills, MI: Greenhaven Press, 2004), pp. 23-33.

Cronin and Ludes Textbook:

Paul R. Pillar, Chapter 5, "Intelligence," (pp. 115-139).

Lesson 3 - Minnesota Smallpox Vaccine Program Case: A Study in Homeland Security Policy

Objectives

1. To analyze a case study that addresses protecting the public from a potential biological weapons attack, planning for and implementing a federal smallpox vaccine program, and coordinating and implementing emergency preparedness across federal, state, and local levels of government.
2. To collaborate with classmates in assessing case study events and key actor decisions and actions and sharing interpretations, assessments, ideas, and conclusions about the case study.
3. To independently write an evaluation summary of the case study with recommendations in a memorandum to a senior policy maker.

Landmarks

1. Read handouts provided by the instructor in advance that address the characteristics and benefits of case studies; and student preparation and involvement for case studies.
2. Take notes while reading the case study very carefully, reflect on events in the case study, and think about appropriate policy and actions for the many case study dimensions.

Discussion Questions

1. What are the most important issues and complexities raised in the case study?
2. What are some lessons that can be extracted from the case study?
3. What course of action should the Minnesota Department of Health (MDH) take regarding Phase 2 and vaccinations for Ramsey County first responders?

Assignments Due

Case Study Evaluation #1 (Memorandum)

Required Readings

Case Study, *"When Prevention Can Kill: Minnesota and the Smallpox Vaccine Program,"* Number C15-03-1709.0, Harvard University, Kennedy School of Government. (32 pp.)

National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Organizing for a Secure Homeland" (pp. 11-14), "Law" (pp. 47-50), "Science and Technology" (pp. 51-54), "Information Sharing and Systems" (pp. 55-58), "International Cooperation" (pp. 59-61), "Conclusion: Priorities for the Future" (pp. 67-69), and "Appendix: September 11 and America's Response" (pp. A-1 to A-4).

Additional Recommended Readings

Third Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: For Ray Downey, December 15, 2001, "Executive Summary" (pp. iii-xi), "Chapter 1. Introduction" (pp. 1-5), and "Chapter III. Improving Health and Medical Capabilities" (pp. 25-34).

Fourth Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: IV. Implementing the National Strategy, December 15, 2002, "Chapter III. Applying Cross-Cutting Themes" (pp. 27-32), "Chapter V. Organizing the National Effort" (pp. 37-50), and "Chapter VI. Improving Health and Medical Capabilities" (pp. 51-67).

Martha Crenshaw, "Counterterrorism Policy and the Political Process," (2001) Chapter 9 in *Terrorism and Counterterrorism: Understanding the New Security Environment* (Guilford, CT: McGraw-Hill/Dushkin, 2004). (pp. 450-458)

Lesson 4 - Weapons of Mass Destruction: Chemical, Biological, Radiological, and Nuclear (CBRNE) Terrorism

Objectives

1. To define "weapon of mass destruction" (WMD).
2. To be familiar with the distinguishing characteristics of chemical, biological, radiological, and nuclear (CBRN) weapons and why they are threats to U.S. national security.
3. To explain the three principal pillars of the *National Strategy to Combat Weapons of Mass Destruction* and the four critical enabling functions that integrate the pillars.
4. To understand what actions are necessary for an effective strategy for biological security that encompasses nonproliferation, deterrence, and defense.
5. To explain the four essential pillars of the national biodefense program outlined in HSPD-10.

Landmarks

1. Terrorism with weapons of mass destruction poses a grave security threat to the U.S., the use of CBRN weapons is possible and probable, and if used, CBRN weapons will cause catastrophic and extensive loss of life and destruction of property.
2. Recognize the value of the first Gilmore Commission report that was published two years before 9-11.
3. Pay attention to the magnitude of the WMD threat, the major actions taken to prevent it and prepare for it, and the tremendous additional efforts necessary to counter and recover from it.

Discussion Questions
1. What are the major challenges confronting the American people and federal, state, and local governments regarding domestic preparedness for CBRN weapons?
2. What aspect of the *National Strategy to Combat Weapons of Mass Destruction* is the most controversial and why?
3. What are the most salient issues for U.S. actions for a biological security strategy?
4. Why and how did the Bush administration make strengthening the nation's defenses against biological weapons a critical national priority?

Required Readings
First Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: I. Assessing the Threat (Gilmore Commission), December 15, 1999, "Executive Summary" (pp. vi-xi), "I. Introduction" (pp. 1-5), and "II. Assessing the Threat: CBRN Terrorism and the Implications for U.S. Security and Preparedness" (pp. 6-39).
National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Defending Against Catastrophic Threats" (pp. 37-40) and "Emergency Preparedness and Response" (pp. 41-45).
National Strategy to Combat Weapons of Mass Destruction, The White House, December 2002. (6 pp.) [Same as HSPD-4, *National Strategy to Combat Weapons of Mass Destruction* (*unclassified version*), December 11, 2002]
Christopher F. Chyba, "Toward Biological Security," *Foreign Affairs*, Vol. 81, No. 3 (May/June 2002): 122-136.
HSPD-10, *Biodefense for the 21st Century*, April 28, 2004. (6 pp.)

Additional Recommended Readings
None

BLOCK 2– HOMELAND DEFENSE

Lesson 5 - U.S. National Security Strategy and National Strategy for Homeland Security

Objectives
1. To be familiar with the three elements, eight goals, and primary themes of the *U.S. National Security Strategy.*
2. To be familiar with the three strategic objectives, six critical mission areas, and four foundations of the *National Strategy for Homeland Security.*
3. To understand Ruth David's three-dimensional strategic framework for homeland security.
4. To defend and critique John Gaddis' view that the *U.S. National Security Strategy* is "the most important reformulation of U.S. grand strategy in over half a century."

Landmarks

1. Identify places in the readings that mention "preemption" or make reference to the concept of preemption and be prepared to discuss it in class.
2. Read the "Executive Summary" and "Introduction" sections of the *National Strategy for Homeland Security* carefully since they form the foundation for this large strategy document.
3. Keep in mind that the Ruth David article first appeared prior to the release of the *National Strategy for Homeland Security*.

Discussion Questions

1. What is the relationship between the *National Security Strategy* and the *National Strategy for Homeland Security*?
2. What are some significant themes that permeate the *National Security Strategy*?
3. Where have you observed evidence of actions that reflect any of the "major initiatives" (for each critical mission area) specified in the *National Strategy for Homeland Security*?
4. How would you modify Ruth David's strategic framework for homeland security?
5. How does the Bush administration's *National Security Strategy* contribute to a grand strategy?

Required Readings

The National Security Strategy of the United States of America, The White House, September 2002. (31 pp.)

National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Executive Summary" (pp. vii-xiii) and "Introduction" (pp. 1-5).

Ruth David, "Homeland Security: Building a National Strategy," *Journal of Homeland Security* (July 2002): 7 pp.

John Lewis Gaddis, "A Grand Strategy of Transformation," *Foreign Policy*, No. 133 (November/December 2002): 50-57.

Additional Recommended Readings

HSPD-1, *Organization and Operation of the Homeland Security Council*, October 29, 2001. (3 pp.)

HSPD-3, *Homeland Security Advisory System*, March 11, 2002. (3 pp.)

Executive Order 13260, *Establishing the President's Homeland Security Advisory Council and Senior Advisory Committees for Homeland Security*, March 21, 2002. (2 pp.)

HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. (2 pp.)

Lesson 6 - NORAD and U.S. Northern Command Roles: Homeland Defense

Objectives

1. To explain Secretary Rumsfeld's intentions and approaches for continuous defense transformation.
2. To be familiar with the basic tenets of the *National Defense Strategy of the United States of America* and the *National Military Strategy of the United States of America*.
3. To understand the mission of North American Aerospace Defense Command (NORAD).
4. To understand the homeland defense mission of U.S. Northern Command (USNORTHCOM).
5. To diagram the "Homeland Security/Homeland Defense Paradigm" model and state examples of activities falling within each sector of the model.
6. To explain Timothy Hoyt's new paradigm for the use of military force since 9-11.

Landmarks

1. Be aware that terminology has been evolving such as "military assistance to civil authorities" (MACA) being changed to "civil support" (CS) and then changed to "defense support to civil authorities" (DSCA).
2. The article by Thomas Goss is very well written and explains the differences between homeland defense and homeland security. Knowing these differences is fundamental to this course.
3. Link concepts in the readings on grand strategy, national security strategy, defense strategy, military strategy, homeland security, homeland defense, and the use of military force since they relate to each other.

Discussion Questions

1. How do the *National Military Strategy* objectives relate to and support the *National Defense Strategy* strategic objectives?
2. What are some emphasis areas that consistently appear in both the *National Military Strategy* and the *National Defense Strategy*?
3. How and where do the NORAD and USNORTHCOM missions relate to the *National Military Strategy* and the *National Defense Strategy*?
4. What are the homeland defense mission categories and what is the nature of them, individually and collectively?
5. What is the significance of the USNORTHCOM mission assurance activities?
6. How are homeland security (HLS), homeland defense (HLD), civil support (CS), and emergency preparedness (EP) distinct and overlapping, what are the relationships among them, and what are examples of each?

Assignments Due

None

Required Readings

Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs*, Vol. 81, No. 3 (May/June 2002): 20-32.

The National Defense Strategy of The United States of America, Department of Defense, March 2005. (20 pp.)

National Military Strategy of the United States of America, 2004. (30 pp.)

U.S. Northern Command's Strategic Vision, September 11, 2003. (21 pp.)

Lt Col Thomas Goss, "Homeland Defense and Homeland Security: Understanding the Military's Role Inside the United States," 2004, submitted to *Joint Forces Quarterly*. (12 pp.)

Cronin and Ludes Textbook: Timothy D. Hoyt, Chapter 7, "Military Force," (pp. 162-185).

Additional Recommended Readings

Steve Bowman, *Homeland Security: The Department of Defense's Role*, Congressional Research Service Report for Congress, CRS Report #RL31615, Updated May 14, 2003. (7 pp.)

Christopher Bolkcom and Steve Bowman, *Homeland Security: Establishment and Implementation of Northern Command*, Congressional Research Service Report for Congress, CRS Report #RS21322, updated August 11, 2003. (6 pp.)

Defense Science Board 2003 Summer Study on DoD Roles and Missions in Homeland Security, Volume I, November 2003. (86 pp.)

Richard H. Kohn, "Using the Military at Home: Yesterday, Today, and Tomorrow," *Chicago Journal of International Law*, Vol. 4, No. 1 (Spring 2003): 165-192.

Lesson 7 - U.S. Northern Command Roles: Defense Support of Civil Authorities

Objectives

1. To understand the defense support of civil authorities (DSCA) mission of U.S. Northern Command (USNORTHCOM).
2. To explain the Posse Comitatus Act, the circumstances under which it applies, and exceptions to it.
3. To understand the significance of maritime security policy and be familiar with the policy contents of HSPD-13, *Maritime Security Policy.*

Landmarks

1. DSCA includes MACA, MSCLEA, and MACDIS. (See question 1.)
2. Statutes and legal considerations bear significantly on the employment of military forces in domestic crises and homeland defense activities. The Posse Comitatus Act limits the use of military forces; however, other laws specify when the Posse Comitatus Act does not apply. Misinterpretations, misunderstandings, and misperceptions about the act abound. Because the act and what is and is not permissible are critical to the mission of USNORTHCOM, it is essential for students to understand the Posse Comitatus Act.
3. Note in the readings when the Posse Comitatus Act does and does not apply to the National Guard.
4. Maritime domain awareness has emerged as one of the priorities for USNORTHCOM.

Discussion Questions

1. Under what circumstances is the defense support of civil authorities (DSCA) mission implemented as military assistance to civil authorities (MACA), military support to civilian law enforcement agencies (MSCLEA), and military assistance for civil disturbances (MACDIS)?
2. What are the constraints, prohibitions, and exceptions for military enforcement of civilian laws according to the Posse Comitatus Act?
3. What are the primary arguments about the Posse Comitatus Act made by Craig Trebilcock and John Brinkerhoff in their articles?
4. What is maritime domain awareness and why is it necessary to have a National Strategy for Maritime Security?

Required Readings

Strategy for Homeland Defense and Civil Support, June 2005. (40 pp.)

Gregory D. Grove, "The U.S. Military and Civil Infrastructure Protection: Restrictions and Discretion under the Posse Comitatus Act," Stanford University, Center for International Security and Cooperation, October 1999. (77 pp.)

Major Craig T. Trebilcock, "The Myth of Posse Comitatus," *Journal of Homeland Security* (October 2000): 5 pp.

John R. Brinkerhoff, "The Posse Comitatus Act and Homeland Security," *Journal of Homeland Security* (February 2002): 8 pp.

HSPD-13, *Maritime Security Policy*, December 21, 2004. (9 pp.)

The National Strategy for Maritime Security, September 2005. (27 pp.)

Additional Recommended Readings

Third Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: For Ray Downey, December 15, 2001, "Chapter VI. Clarifying the Roles and Missions of the Military" (pp. 46-54).

Fourth Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic

Response Capabilities for Terrorism Involving Weapons of Mass Destruction: IV. Implementing the National Strategy, December 15, 2002, "Chapter IX. Establishing Appropriate Structures, Roles, and Missions for the Department of Defense" (pp. 86-103).

Paul Schott Stevens, *U.S. Armed Forces and Homeland Defense: The Legal Framework* (Washington, D.C.: Center for Strategic and International Studies Press, October 2001). (29 pp.)

Colonel Steven J. Tomisek, "Homeland Security: The New Role for Defense," *Strategic Forum*, No. 189 (February 2002): 1-8.

Jeffrey H. Norwitz, "Combating Terrorism: With a Helmut or a Badge," *Journal of Homeland Security* (August 2002): 10 pp.

Lesson 8 - Cyber Terrorism and Terrorism Against Critical Infrastructure

Objectives

1. To know the U.S. critical infrastructure sectors and key assets and the meaning of critical infrastructure protection (CIP).
2. To be familiar with the three strategic objectives, statement of national policy, eight guiding principles, and government and private sector responsibilities of the *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets*.
3. To be familiar with the statement of national policy, three strategic objectives, themes, and five national priorities of the *National Strategy to Secure Cyberspace*.
4. To understand the importance of effective CIP information-sharing partnerships, relationships, and actions.
5. To be familiar with the purpose, organization, and scope of the *Interim National Infrastructure Protection Plan*.

Landmarks

1. Think about how the three strategy documents assigned as readings are related to each other.
2. Take note of the common themes among the three strategy documents assigned as readings.

Discussion Questions

1. Why are critical infrastructures and key assets vulnerable, why must they be protected, and what is the status of CIP efforts?
2. What provisions in HSPD-7 apply to the Department of Defense?
3. According to the GAO report in the assigned readings, what are the major challenges to effective information sharing between industry sectors and government and what actions have been and need to be taken to address those challenges?
4. What is your assessment of the *Interim National Infrastructure Protection Plan*?

Required Readings

National Strategy for Homeland Security, Office of Homeland Security, The White House, July 2002, "Protecting Critical Infrastructure and Key Assets" (pp. 29-35).

National Strategy to Secure Cyberspace, The White House, February 2003, "Executive Summary" (pp. vii-xiii), "Introduction" (pp. 1-4), "Cyberspace Threats and Vulnerabilities: A Case for Action" (pp. 5-11), "National Policy and Guiding Principles" (pp. 13-17), "Conclusion: The Way Forward" (pp. 53-54), and "Actions and Recommendations Summary" (pp. 55-60).

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, The White House, February 2003, "Executive Summary" (pp. vii-xii), "Introduction" (pp. 1-4), "The Case for Action" (pp. 5-10), "National Policy and Guiding Principles" (pp. 11-13), "Conclusion" (pp. 81-82).

HSPD-7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003. (9 pp.)
U.S. General Accountability Office, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO Report, Number GAO-04-780, July 2004. (63 pp.)
Department of Homeland Security, *Interim National Infrastructure Protection Plan* (Washington, D.C.: Department of Homeland Security, February 2005). (pp. 1-11)

Additional Recommended Readings

Third Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: For Ray Downey, December 15, 2001, "Chapter V. Enhancing Cyber Security" (pp. 41-45).
Fourth Annual Report to The President and The Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction: IV. Implementing the National Strategy, December 15, 2002, "Chapter VIII. Improving the Protection of Our Critical Infrastructure" (pp. 77-85).
HSPD-9, *Defense of United States Agriculture and Food*, January 30, 2004. (6 pp.)

Lesson 9 - 9/11 Pentagon Emergency Case Study and U.S. Grand Strategy

Objectives

1. To analyze a case study that addresses the unprecedented emergency response operation at the Pentagon on September 11, 2001.
2. To collaborate with classmates in assessing case study events and key actor decisions and actions and sharing interpretations, assessments, ideas, and conclusions about the case study.
3. To independently write an evaluation summary of the case study with recommendations in a memorandum to a senior policy maker.
4. To understand the role of the National Incident Management System (NIMS) and the National Response Plan (NRP) for domestic incident management.
5. To describe the purpose, concepts, principles, and components of the NIMS.
6. To describe the purpose, scope, applicability, and organization of the NRP.
7. To understand the arguments for a U.S. grand strategy against terrorism.

Landmarks

1. Read handouts provided by the instructor in advance that address the characteristics and benefits of case studies; and student preparation and involvement for case studies.
2. Take notes while reading the case study very carefully, reflect on events in the case study, and think about appropriate policy and actions for the many case study dimensions.
3. HSPD-5, *Management of Domestic Incidents*, directs the development of the NIMS and the NRP which result in vastly improved coordination among federal, state, and local organizations to help save lives and protect communities by increasing the speed, effectiveness, and efficiency of incident management.
4. Creating an effective grand strategy is the major theme and thread that runs through the Cronin textbook. The final two chapter readings assigned for this week from the Cronin textbook synthesize that theme and many of the arguments made in course readings and class discussions.

Discussion Questions

1. What are the most important issues and complexities raised in the case study?
2. What are some lessons that can be extracted from the case study?
3. How do events in the case study relate to contents of the NIMS and the NRP?

4. What provisions in HSPD-5 relate to the DoD?

Required Readings

Case Study, *"Command Performance: County Firefighters Take Charge of the 9/11 Pentagon Emergency,"* Number C16-03-1712.0, Harvard University, Kennedy School of Government. (44 pp.)

HSPD-5, *Management of Domestic Incidents*, February 28, 2003. (5 pp.)

Department of Homeland Security, *National Incident Management System* (Washington, D.C.: Department of Homeland Security, March 1, 2004). (pp. v-x, 1-6)

Department of Homeland Security, *National Response Plan* (Washington, D.C.: Department of Homeland Security, November 2004). (pp. i-iii, ix-xvi, 1-5, 41-43)

Cronin and Ludes Textbook:

Daniel Goure, Chapter 11, "Homeland Security," (pp. 261-284).

Audrey Kurth Cronin, "Conclusion, Toward an Effective Grand Strategy," (pp. 285-299).

Additional Recommended Readings

9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, Chapter 12, "What to Do? A Global Strategy," (pp. 361-398).

Lesson 10 - National Guard

Objectives

1. To understand the role and missions of the National Guard for federal mobilization and homeland defense.
2. To differentiate Title 10, Armed Forces, and Title 32, National Guard.
3. To explain contemporary issues facing the National Guard.
4. To know how HSPD-8, *National Preparedness*, is a companion to HSPD-5, *Management of Domestic Incidents*.

Landmarks

1. Throughout the readings, there is consistent reference to a need for the National Guard to acquire more capabilities and take on greater responsibilities for homeland security.
2. Knowing the differences between National Guard Title 10 and Title 32 roles is fundamental to the course.

Discussion Questions

1. What are the common themes and arguments in the Jack Spencer/Larry Wortzel and John Brinkerhoff articles?
2. For the Jack Spencer/Larry Wortzel and John Brinkerhoff articles, which makes the most compelling case and why?
3. What are the most pressing issues for the National Guard in the short-term and long-term and how should they be addressed?
4. What provisions in HSPD-5 and HSPD-8 apply to the Department of Defense?

Required Readings

Jack Spencer and Larry M. Wortzel, "The Role of the National Guard in Homeland Security," *Journal of Homeland Security* (April 2002): 7 pp.

John R. Brinkerhoff, "The Changing of the Guard: Evolutionary Alternatives for America's

National Guard," *Journal of Homeland Security* (May 2002): 28 pp.

U.S. General Accountability Office, *Reserve Forces: Actions Needed to Better Prepare the National Guard for Future Overseas and Domestic Missions*, GAO Report, Number GAO-05-21, November 2004. (38 pp).

HSPD-8, *National Preparedness*, December 17, 2003. (6 pp.)

Additional Recommended Readings

9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States, 2004, Chapter 13, "How To Do It? A Different Way of Organizing the Government," (pp. 399-428).