

# *Appendix B*

## **Syllabus of Qualifying Examinations** **PhD in Engineering with a focus in Security**

### **Cyber Security Part**

*Computer Communications*  
*Fundamentals of Computer/Network Security*  
*Applied Cryptography for Secure Communication*

### **Physical Security Part**

*Probability and Statistics*  
*Vision, Image, and Sensor Processing*  
*Security Standards*  
*Protection of Critical Infrastructures*

### **Homeland Security Part**

*Homeland Security and Defense*  
*Understanding the Threats*

# *Computer Communications*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

**Reference course: CS522 Computer Communications, College of EAS, UCCS**

**Created by Prof. Xiaobo Zhou, 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", 4<sup>th</sup> 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: CS591 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 to 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," 2<sup>nd</sup> 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," 3<sup>rd</sup> Edition, Prentice Hall, **ISBN-13:** 978-0132380331, 2006.
- Charlie Kaufman, Radia Perlman, Mike Speciner, "Network Security: Private Communication in a Public World", 2<sup>nd</sup> 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/Prevention 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](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](http://www.dwheeler.com/secure-programs/Secure-Programs-HOWTO/index.html), 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 by Oskar Andreasson. <http://iptables-tutorial.frozentux.net/iptables-tutorial.html>
- IDS:
  - Snort Users Manual [http://www.snort.org/docs/snort\\_htmanuals/htmanual\\_280/](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](http://sourceforge.net/docman/display_doc.php?docid=2078&group_id=3130)
- Penetration testing, *By Stephen Northcutt, Jerry Shenk, Dave Shackelford, 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: CS592 *Applied Cryptography for Secure Communication*,  
College of EAS, UCCS**

**Created by Prof. Jugal Kalita, last updated February 2008**

---

---

### **Description:**

Cryptography is an enabling technology for protecting confidentiality and integrity of the data in today's information systems. Applied cryptography for secure communication deals with applying the cryptography techniques for achieving desirable security properties in communications, including authenticity of data and identity of users and system component, encryption of data, providing non-repudiation, and ensuring anonymity and accountability.

This examination covers the basics of applied cryptography for secure communication. Students should be able to analyze the needs in a suggested secure communication scenario and propose the proper cryptography based solutions.

### **Reference Textbooks and Articles**

- "Cryptography and Network Security," by Behrouz A. Forouzan, McCaw-Hill, 2008. ISBN 978-0-07-287022-0
- Chapter 8 of "Computer Network" by Tanenbaum
- A. Shamir, "How to Share a Secret", Communication of the ACM, Vol. 22, No. 11, pp. 612-613, Nov. 1979.

Alternatives:

- "Cryptography and Network Security: Principles and Practices," Third Edition. William Stallings, Prentice hall, ISBN0-13-091429-0.
- Niels Ferguson and Bruce Schneier, "Practical Cryptography", Wiley Publishing Inc., 2003.
- ICOSA Guide to Cryptography by Randal K. Nicholls, 1999.
- Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, 1996, CRC Press.
- Introduction Cryptography with Coding Theory, Wade Trappe and Lawrence C. Washington.

### **Covered Topics**

- Classical cryptographic algorithms: Caesar, Monoalphabetic and Vigenere Ciphers.
- Symmetric algorithms: DES and Variation, AES, and Modes of Operation of Symmetric Ciphers
- Public key cryptographic algorithms: RSA
- Key management and other issues, elliptic cryptography
- Hash algorithms.

- Digital signatures and authentication protocols.
- Share Secret Scheme.
- Utilize OpenSSL for creating certificates and encryption.
- Set up secure web access with basic password authentication and mutual digital certificate based authentication.

### **Background Expected**

- Integer arithmetic
- Modular arithmetic
- Algebraic structures

# *Probability and Statistics*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

Reference course: Psy 581 Statistics Methods, College of LAS, UCCS

Created by Prof. Terry Boulton, last updated February 2008

<http://vast.uccs.edu/~tboulton/prob>

---

### ***Probability Topics:***

- Individual Chapters from [Introduction to Probability by Frinstead and Snell](#)

1. [Discrete Probability Distributions](#) including:
  - Simulation of Discrete probabilities
  - Discrete Probability Distribution
2. [Continuous Probability Densities](#)
  - Continuous Density Function
  - Simulation of continuous Probabilities
3. [Combinatorics](#)
  - Permutations
  - Combinations
4. [Conditional Probability](#)
  - Discrete Conditional Probability
  - Continuous Conditional Probability
  - Paradoxes
5. [Important Distributions and Densities](#)
  - Distributions: Uniform, Binomial (positive and negative), Geometric, Guassian, Normal
  - Poisson distribution Hypergeometric Geometric distribution, Benford distribution
  - Exponential, Normal Densities, Rayleigh, Cauchy, Chi-Squared Densities
  - Transformation of variables and Transformation of densities
6. [Expected Value and Variance](#)
  - Expected value
  - Variance of Discrete Random Variables
  - Variance of Continuous Random Variables
7. [Sums of Independent Random Variables](#)
  - Sums of Discrete Random Variables
  - Sums of Continuous Random Variables
8. [Law of Large Numbers](#)
  - Law of large numbers for Discrete Random Variables
  - Law of large numbers for Continuous Random Variables
9. [Central Limit Theorem](#)
  - Bernoulli Trials
  - Discrete Independent Trials
  - Continuous Independent Trials

The following may also be useful in your probability study if you use the above book:

[Index](#)

### [Answers to odd-numbered exercises](#)

---

## ***Statistics***

(Drawing significantly from [Dave Lanne's Online hyperstat text](#) (all topics available from that site). Topic should exist in any standard statistics text.

1. Basic statistics:
  1. About descriptive statistics
  2. About inferential statistics
  3. Variables
  4. Parameters
  5. Statistics
  6. Summation notation
  7. Measurement scales
2. Describing Univariate Data
  - Central Tendency including Mean, Median, Mode, Trimean, Trimmed Mean
  - Spread including: Range, Semi-Interquartile Range, Variance, Standard Deviation
  - Shape including: Skew, Kurtosis
  - Graphs including: Frequency Polygons, Histograms, Stem and Leaf Displays, Box Plots
3. Describing Bivariate Data
  - Scatterplots
  - Introduction to Pearson's Correlation
  - Computational formula for Pearson's Correlation
  - Example values of  $r$
  - Effect of restricted range on Pearson's Correlation
  - Effect of linear transformations on Pearson's Correlation
  - Spearman's  $\rho$
4. Confidence Intervals
  - Mean,  $\sigma$  known
  - Mean,  $\sigma$  estimated
  - General formula
  - Difference between means of independent groups,  $\sigma$  known
  - Difference between means of independent groups,  $\sigma$  estimated
  - Linear combination of means from independent groups
  - Pearson's correlation
  - Difference between correlations
  - Proportion
  - Difference between proportions
5. The Logic of Hypothesis Testing
  - Ruling out chance as an explanation
  - The null hypothesis
  - Steps in hypothesis testing
  - Why the null hypothesis is not accepted
  - The precise meaning of the  $p$  value
  - At what level is  $H_0$  really rejected?
  - Statistical and practical significance

- Type I and II errors
- One- and two-tailed tests
- Confidence intervals and hypothesis testing
- Following a nonsignificant finding
- 6. Testing Hypotheses with Standard Errors
  - General formula
  - Tests of  $\mu$ ,  $\sigma$  known
  - Tests of  $\mu$ ,  $\sigma$  estimated
  - $\mu_1 - \mu_2$ , independent groups,  $\sigma$  estimated
  - $\mu_1 - \mu_2$ , dependent means,  $\sigma$  estimated
  - Linear combination of means, independent groups
  - Tests of Pearson's correlation
  - Differences between correlations
  - Proportions
  - Differences between proportions
- 7. Power and Factors affecting power
  - what is statistical power
  - Size of difference between means
  - Significance level
  - Sample size
  - Variance
  - Other factors
- 8. Introduction to Between-Subjects ANOVA
  - Preliminaries
  - ANOVA with 1 between-subjects factor
    - Two estimates of variance
    - The significance test in ANOVA
    - Partitioning the sums of squares
    - Computational methods
  - Tests supplementing ANOVA
    - Introduction
    - All pairwise comparisons among means
      - Introduction
      - All pairwise t-tests
      - Fisher's LSD
      - Recapitulation and recommendations
      - Example calculations
    - Comparing means with a control
    - Specific comparisons among means
      - Overview
      - Computing comparisons
      - Multiple comparisons
      - Orthogonal comparisons
      - Trend analysis
  - Formal model
  - Expected mean squares
  - Reporting results
- 9. Prediction
  - Introduction

- Standard error of the estimate
- Partitioning the sums of squares
- Confidence intervals and significance tests for correlation and regression
- Multiple regression
  - Introduction
  - Significance tests
  - Shrinkage
  - Measuring a variable's importance
- Regression toward the mean
- Exercises

#### 10. Chi Square

- Testing Differences between sample proportion and population proportion
- Computing Chi Square test of Independence
- key assumption of the chi square test of independence

# *Image, Vision, and Sensor Processing*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

Reference courses: CS 505 and CS584, College of EAS, UCCS

Created by Prof. Terry Boulton, last updated February 2008

<http://vast.uccs.edu/~tboulton/CS505/> and <http://vast.uccs.edu/~tboulton/CS584/>

---

### **Image and Sensor Processing Description:**

This course will be a mixture of the underlying principles of image processing with a lot of the issues in making it practical. It will examine computational and theoretical aspects of image processing including representations, image formation/sensing, sampling theory, reconstruction/interpolation, warping and geometric transforms, filtering, wavelets and FFTs as well as higher level image processing concepts including segmentation, noise removal, and feature/target detection and tracking. While focused on images for examples, most of the computational techniques apply across many areas of signal processing. At least 1 assignment will be doing real-time image processing in C/C++ and one will be a spectral analysis in Matlab.

Overall I expect course will have 3-4 software assignments (maybe teams, maybe no team depends on the size of the class). No regular homework but maybe 1-2 quizzes. Largely lecture but some time there will be discussion oriented classes as well. All students will give 1-2 presentations (depending on class size).

### **Reference Textbooks**

- Image Processing in C by D. Phillips
- Feature Extraction & Image Processing Mark S. Nixon and Alberto S. Aguado, <http://www.ecs.soton.ac.uk/~msn/book/>
- And a free/online one: [Hypermedia Image Processing Reference](#) by R.B. Fisher, S. Perkins, A. Walker, E. Wolfart. John Wiley and Sons, 1996
- A useful reference may also be: Digital Image Processing Using MATLAB - by Gonzalez, Woods, and Eddins, Prentice Hall,

### **Projects**

- (1) In <http://www.vast.uccs.edu/~tboulton/CS505/IMGS> there are 7 images (one pretty large) to which you are to use FFT analysis to try to remove the distortions/noise. For each one you are to do an openCV, Matlab or other program to "correct it". It is not sufficient to turn in the images, I want the steps you undertake, the code you produce and why that is the right

solution (as comments in code is fine). If you make assumptions or discoveries along the way, make them clear in comments in the code both what they are and how you reached them. For 25 bonus points, do at least 2 images, one of which should be the large image, in both openCV and matlab and discuss the timing differences and the ease of coding.

(2) This project is to do some applied computational image processing, building on something from the course. The subject of the project is up to you, but when thinking about the scale, keep in mind the expected effort is on the order of 50-60 hrs for programming and writing the report. The platform is up to you. The language is up to you. But the project has a number of constraints:

- Your project cannot be just a reimplement of something in a common image processing library. It may provide the same functionality, but must do it in a novel manner. Or it can provide a novel feature. Or it can moderately improve the performance of an existing implementation. It must add value, either in novelty or performance.
- You may use libraries, but must write at least most of the "significant" functions for your project. The description of the functionality you will implement yourself must be in your project outline, and refined in your interim report.
- Your outline should describe the problem to be solved, the main image processing steps you see, how you will measure your progress, and the platform/libraries to be used.

Your "testing" must involve at least a dozen images/examples to validate your project.

---

---

## **Vision and Sensor Processing Description:**

The objective of this course is to convey the basic issues in computer vision and major approaches that address them. After completing the course, the students may expect to have the knowledge needed to read and understand the more advanced topics and current research literature, and the ability to *solve* basic industrial "vision" problems. The course will have plenty of hands-on experience building exercises. This course is *NOT* designed to be a "cookbook" course that gives just a survey of the methods needed in "practice" and will it not cover "commercial" systems in any detail. Vision is a very broad topic and this course is a beginning, not an end.

## **Textbooks**

Required:

[\*Computer Vision : A Mordern Approach, D. Forsyth and J. Ponce\*](#), Prentice-Hall, 2001

And Papers, manuals and web documents as assigned.

## References

1. *Computer Vision*, [D. Ballard](#) and [C. Brown](#), Prentice-Hall, 1982. and its available [online \(for free\)](#)
2. *Computer and Robot Vision vol. 2*, R. Haralick and L. Shapiro, Addison-Wesley, 1992
3. *Robot Vision*, [B.K.P. Horn](#), MIT Press, 1986
4. *Three-Dimensional Computer Vision*, [O. Faugeras](#), MIT Press, 1993
5. *A Guided Tour of Computer Vision*, V. S. Nalwa, Addison Wesley, 1993
6. *Vision*, David Marr, Freeman, 1982

## Prerequisites

1. Students must be able to program in C++.  
CS 145 or equivalent - Data Structures, good programming skills.  
CS306 (OO programing in C++). recommend
2. Ability to convert vague problem descriptions and informatl specifications into computer algorithms. Recommended: CS330 Software Engineering
3. Basic Mathematics - Good facility with calculus and analytical solid geometry is essential. If you have not used them for several years, you must be prepared to spend some time to review them (and the assignments may take more than the allotted time). Undergraduate knowledge of linear algebra, matrix theory and elementary probability theory will also be helpful.

## Course Topics

Following is a list of topics expected to be covered, in anticipated order, and with expected time to be spent on them. This list is intended to be only indicative, the actual topics, the order and the time may vary somewhat depending on various factors including student interests and preparation.

1. **Introduction (1 week)**  
Background, requirements and issues, human vision.  
For Week of 1/26 read chapters 1,2. Download and read about [opency](#).
2. **Intro to OpenCV (1 class)**  
Notes and manual
3. **Image formation (1 week)**  
Radiometry and color, (Ch 4 and 6)
4. **Image segmentation (2 weeks)**  
Edge and line finding, region segmentation
5. **Grouping (2 weeks)**  
Background Subtraction, Morphology, Connected Components grouping
6. **Shape analysis and object recognition (1-2 weeks)**  
Hough, fitting Shape representation and matching
7. **Activity Undrstanding (1 week)**  
Tracking and inference of human activity from image sequences.
8. **Understanding geometry (1 weeks)**  
Camera Calibration, pose estimation

9. **Multi-view Geometry (1 weeks)**  
Shape from stereo and motion, motion tracking
10. **Applications survey (1 week)**  
Industrial, navigation, mapping, multimedia

## ***Projects***

The course will have numerous programming assignments. Assignments can be done on UCCS machines or on your own. Assignments can be done in either windows or Linux. Web cameras will be available (Depending on enrollment either for the semester or on a daily basis). Assignments and class handouts will be available here.

All "software related" assignments in this class is to be done on a two person team basis. Each team assignment will be given a total number of points. Based on the teams reports, each team will achieve a total number of points. These points will be shared, not necessarily equally, among team members.

You are bound by the rules of [CU-Colorado Springs Academic Honor Code](#) Except for sharing information between members of the same team, any collaboration, plagiarism or any other offense listed therein is consider cheating and will be referred to the disciplinary committee. Even though assignments are team assignment, sharing materials or even detailed discussions of solution techniques, between teams, is considering CHEATING. Make sure you protect your files, if someone copies from you, you are both responsible. If in assignments you "borrow" code from places other than our text or openCV, even small segments of code, you need to give proper acknowledgement in your code. I reserve the right to deny any student from being graded under the homework weighted option, independent of the handling of their case by the disciplinary committee.

1. Software assignment #1. Using OpenCV, process your "picture" (i.e. photo from last week) to produce:
  1. A blurred facial image, 3 levels of blurring.
  2. A detected/localize face on all 4 (orig + 3 blurred images)
  3. and edge image with 3 different levels of "edgeiness", applied to all 4 images (i.e. 12 different images).
  4. 3 different levels of "segmented" image
  5. Write a openCV program that loads an image, blurs it, adds random noise, detects the face and computes the errors of the detection/localization. Run it for a range of parameters and report the errors. To facilitate comparison you should use both your picture and my picture (from my web page). You should explain how you define and computed the error in detection/localization.

Your team will turn in your results by posting them on a web-page and emailing me the URL.

Note: people have asked if you can use Hawk. The answer is yes but I strongly suggest you try to get the Compiler-version going in your environment. The next assignment is video based and it is hard to do it in Hawk.

2. Software assignment #2 (teams allowed). Choose an application (e.g. hand-recognition, or part inspection) not already implemented in openCV (e.g. face detection is not allowed) and do the following:
  0. Do some image "normalization"/filtering to reduce noise improve dynamic range (may be before or after color work below).
  1. Develop a color-based algorithm to approximately locate the object
  2. then apply a "correlation-based" template matching to locate features for your object (normalized correlation is allowed)
  3. Test the system with at least 20 different "examples" of the input with varying illumination. If possible define and measure the "error" as a function of illumination variations.
  4. and display/save the results.
  5. generate a "report" on the results of your experiment
  6. 30pts extra credit for a near-real-time implementation (say < 150ms per frame) that does this on video streams.

You are encouraged to find a paper in the literature related to your algorithm and see if you can implement the key ideas of that paper. Include proper citations in your report.

If you don't have an application in mind and you would like to help out on our research we can have teams working on the same application (detection and location of fingers/creases on the hand).

3. Software assignment #3 (teams allowed).
  - o Implement Union-find based Connected Components. Output a list of regions with basic properties (area, Bbox, average gray value, gray variance) and a "colored" image showing the results. Test as basis for background-subtraction using 2 different "scenes" with 3 different thresholds.
  - o Implement Quasi-connected Components. Output a list of regions with basic properties (area, Bbox, average gray value, gray variance) and a "colored" image showing the results. Test as basis for background-subtraction using 2 different "scenes" with 3 different thresholds.
  - o Implement basic Component-Morphology allowing pruning of components based on properties. If practical allow pruning before the "relabeling" phase so only the pruned objects are left in the image.
  - o Make one of CC or QCC fast/efficient and in the style of opencv.
  - o Use both CC and QCC to detect the color targets you used in software assignment #2 and compare with the results of the segmentation you did there.

Extra credit:

- o 5pts Extend your union-find to compute properties (like area, Bbox, average, variance) as it does the union steps instead of computing them afterward.
- o 5pts Compare QCC with morphology applied to basic thresholding and CC.

- 10pts Extend QCC to have "temporal" overlap, using a previous parent image with labels which effects the label generation, i.e. keep the same label if the component in this time frame overlaps component in previous time frame.
- 10pts Make a multi-channel (RGB) QCC with 3 low and 3 high thresholds.
- 15pts Make your QCC use multiple scales and explain how it works across scales.

As before prepare a web-page with the result (and email me the code).

4. Software assignment #4 (teams allowed). Part 1:
  - Using OpenCV implement both a Kalman Filter and Condensation tracking syntehtic data where you define the object, motion and noise models (algebraically) and simulate the data then the tracking and then compute formal error and performance measures.
  - Test simple motion (velocity+acceleration model) with noise data drawn from a two different "unimodal" (at most one guassian) distributions,
  - Test model with  $N \geq 3$  targets both moving with vel+accel.

As before prepare a web-page with the result (and email me the code).

Your report (and code comments) should discuss the models used why/How Kalman/Condensation applies.

Your report should discuss how you addressed the data association problem.

Your grade depends on good design/implementation, use of the library and explanation, Not in choosing a model for which Kalman/Condensation tracking works well.

Part 2. Extend your solution to Part 1 to include a "parametric" motion involving multiple constained "parts" (e.g. a simple human model or multiple targets contrained by connections).. Your report (and code comments) should discuss the models and how you implemented it. Discuss its physical plausabiity. Discuss why/how Kalman/Condensation applies, in particular how you developed your dynamic motion model matrixices.

Your report should discuss how you addressed the data association problem. Extra Credit (50 pts) Due by May 10. Using OpenCV, choose either the Kalman Filter or Condensation tracking, and apply it to tracking on real video data. You also need to "segment" to find the data and have some way to

As before prepare a web-page with the result (and email me the code). For examples of condensation in use see: <http://www.stanford.edu/~jbrasket/cs223b/project/>  
<http://www.robots.ox.ac.uk/~misard/condensation.html>

# *Security Standards*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

**Reference courses: CS 613, College of EAS, UCCS**

**Created by Prof. Terry Boulton, last updated February 2008**

<http://vast.uccs.edu/~tboulton/CS613/>

---

### **Security Standards**

1. [Army Field Manual 3-19-30 Physical Security](#) (313 pages including appendices)  
This manual provides a good overview of physical security issues from fences to sensors to training of personnel.
2. [Director of Central Intelligence Directive 1/21: Manual For Physical Security Standards For Sensitive Compartmented Information Facilities \(SCIF\)](#) (66 Pages)  
This manual assumes basic knowledge of physical security and provides details on the added security needed for a secured (classified) facility.
3. In the modern physical security, "ID" is a major issue. FIPS 201 (Federal Information Processing Standards Publication 201) is a United States federal government standard that specifies [Personal Identity Verification \(PIV\)](#) requirements for Federal employees and contractors, mandated by Homeland Security Presidential Directive 12. FIPS 201 incorporates three technical publications specifying several aspects of the required administrative procedures and technical specifications that may change as the standard is implemented and used. NIST Special Publication 800-73, "Interfaces for Personal Identity Verification" specifies the interface and data elements of the PIV card; NIST Special Publication 800-76, "Biometric Data Specification for Personal Identity Verification" specifies the technical acquisition and formatting requirements for biometric data of the PIV system; and NIST Special Publication 800-78, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" specifies the acceptable cryptographic algorithms and key sizes to be implemented and used for the PIV system. You are responsible for the PIV standards in particular for approximately 220 pages of reading:
  - o [FIPS201 \(updated\)](#) (91 pages)
  - o [NIST SP800-76 Biometric Data Specification for Personal Identity Verification](#) (33 pages)
  - o [NIST SP800-73 Interfaces for Personal Identity Verification](#) (71 pages)
  - o [SP 800-78-1](#) - Cryptographic Algorithms and Key Sizes for Personal Identity Verification, (20 pages)
  - o [SP 800-104](#) - A Scheme for PIV Visual Card Topography, (11 pages)
4. Security standards are not all for government facilities. The [North American Electric Reliability Corporation \(NERC\)](#) is a nonprofit corporation designed to "ensure that the bulk electric system in North America is reliable, adequate and secure." As the federally designated Electric Reliability Organization (ERO) in North America, NERC maintains comprehensive reliability standards that define requirements for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection (CIP)

Cyber Security Standards, which are intended to ensure the protection of the Critical Cyber Assets that control or effect the reliability of North America’s bulk electric systems.

In 2006, the [Federal Energy Regulatory Commission \(FERC\)](#) approved the Security and Reliability Standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system.

[Table A-1](#) lists the eight standards and a brief description of each standard.

**Table A-1 CIP Standards**

<b>Standard Number</b>	<b>Topic</b>	<b>Purpose/Description</b>
<a href="#">CIP-002-1</a>	Critical Cyber Assets	Define and document the Critical Assets and the Critical Cyber Assets
<a href="#">CIP-003-1</a>	Security Management Controls	Define and document the Security Management Controls required to protect the Critical Cyber Assets
<a href="#">CIP-004-1</a>	Personnel and Training	Define and Document Personnel handling and training required to protect Critical Cyber Assets.
<a href="#">CIP-005-1</a>	Electronic Security	Define and document logical security perimeter where Critical Cyber Assts reside and measures to control access points and monitor electronic access.
<a href="#">CIP-006-1</a>	Physical Security	Define and document Physical Security Perimeters within which Critical Cyber Assets reside.
<a href="#">CIP-007-1</a>	Systems Security Management	Define and document system test procedures, account and password management, security patch management, system vulnerability, system logging, change control and configuration required for all Critical Cyber Assets.
<a href="#">CIP-008-1</a>	Incident Reporting and Response Planning	Define and document procedures necessary when Cyber Security Incidents relating to Critical Cyber Assets are identified.
<a href="#">CIP-009-1</a>	Recovery Plans	Define and document Recovery plans for Critical Cyber Assets.

5. If you are still awake after all of that and just looking for more fun reading you can try (but are not required to know) the standard for

[The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC/225/Rev.4](#)

# *Protection of Critical Infrastructures*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

**Reference course: INFS 682 Protection of Critical Infrastructures, UCCS**

**Created by Dr. Bill Ayen, last updated February 2008**

---

**Course Bulletin Description:** Course introduces the set of critical infrastructures, with emphasis on threats, vulnerabilities, and information infrastructures. The principles of systems engineering with emphasis on risk-based decision making and systems thinking will be presented. A term project is required.

### **Expanded Description:**

Protecting critical infrastructures is a key requirement for homeland defense and homeland security. Critical infrastructures have direct and indirect relationships with each other. The legal, regulatory, and economic environments affect in some real important ways the structure of and vulnerabilities of the critical infrastructures. Historically protecting critical infrastructures has not been a major focus of America's policies. Since a large percentage of the critical infrastructure assets are privately owned, the ability of the Federal government through legislation or regulation to require investment in protecting of critical infrastructures is limited.

This course will explore the background of critical infrastructures and the interplay of legal, regulatory, and economic forces that have created their current state. An approach called Model-Based Vulnerability Analysis (MBVA) will be introduced through which a critical infrastructure sector or a portion of a sector can be analyzed to determine vulnerabilities and then strategies for allocating resources to reduce vulnerabilities and risk can be determined. A subset of the critical infrastructures will be analyzed in detail using the MBVA approach. Finally, each student will complete a term project that analyzes one of the critical infrastructures and will present the results in a project paper and presentation.

### **Course Objectives:**

- Be able to understand the legal, regulatory, and technical architecture of the principal critical infrastructure sectors in the US
  - Understand how each sector runs
  - Know the major components, vulnerabilities, and threats for each sector
- Know the principles behind and the steps in the Model-Based Vulnerability Analysis (MBVA) approach to developing strategies for protecting critical infrastructures
- Be able to perform MBVA on a critical infrastructure sector
- Understand the importance of protecting critical infrastructures in sectors that pertain to your profession.

### **Reference Textbook:**

Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Ted G. Lewis, Naval Postgraduate School, Wiley, 2006.

**Course Readings:**

- The syllabus includes the textbook readings assigned for each class meeting. Each student is expected to have read each of the **required** readings prior to the class where it will be discussed.
- A CD with an additional set of reference readings and updated software will be distributed.
- Specific reading assignments in addition to the text will be made during the term.

**Course Notes:**

- Copies of slides used in lectures and other information will be posted on the e-Course course web site the week prior to the lecture.
- Weekly exercises will be posted during the week prior to the due date.

**Exercises:**

- Most weeks an exercise will be assigned to reinforce the material in the lecture for that week and/or prepare the student for the next week's lecture. More detailed requirements will be given in each exercise description.
- Grades will be assigned based on correctness and the overall quality of the effort.

# *Homeland Security and Defense*

## **Syllabus of Qualifying Examination**

### **PhD in Engineering with a focus in Security**

**Reference course: PAD595 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 required 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 21<sup>st</sup> Century, Major Themes and Implications*, Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21<sup>st</sup> Century, U.S. Commission on National Security/21<sup>st</sup> 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 21<sup>st</sup> Century, U.S. Commission on National Security/21<sup>st</sup> 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/21<sup>st</sup> 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 21<sup>st</sup> 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 Bolcom 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 Helmet 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).

# *Understanding the Threats*

## **Syllabus of Qualifying Examination**

**PhD in Engineering with a focus in Security**

**Reference course: PAD598 Understanding the Threats, UCCS**

**Created by Center for Homeland Security (CHS), last updated February 2008**

---

### **I. COURSE DESCRIPTION.**

This course presents an overview of threats to United States security. Primary emphasis is placed on understanding the nature and depth of catastrophic and disruptive terror-based threats from non-state and state-supported entities. Supporting topics will include the history and psychology of terrorism; ideological, religious, economic and cultural issues; terror implications of weapons of mass destruction; the nexus of multiple threat sources; and other non-conventional threats to the United States. The course will also review traditional, irregular, and asymmetric threats from nation-state competitors as part of a holistic approach to national defense. Successful completion of course requirements will provide understanding of the multi-dimensional nature of current and future security challenges and an analytical baseline to support counter-threat initiatives.

### **II. EDUCATIONAL OUTCOMES/COURSE OBJECTIVES.**

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. Increase your knowledge and understanding of the various threats to national security.
2. Familiarize you with the growing body of literature on homeland defense and security, and threats associated.
3. Enable you to gain a conceptual and experiential grounding in the complex environment, multiple challenges, and potential interdependent nature of threats facing domestic leaders.
4. Improve your ability to identify, critically analyze, and forcefully articulate threats to North America, and make policy recommendations to domestic leadership.
5. Enhance your ability to listen and communicate accurately and precisely and to work effectively with others on the nature of threats facing the U.S.
6. Further prepare you as effective leaders and managers in homeland defense and homeland security 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.

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. REFERENCING TEXTBOOKS AND MATERIALS.**

##### **A. Required Texts.**

Emerson, Steven (2006). "Jihad Incorporated: A Guide to Militant Islam in the US". New York: Prometheus Books, ISBN: 978-1-59102-453-8.

German, Mike (2007). "Thinking Like a Terrorist". Washington, D.C.: Potomac Books, ISBN: 978-1-59797-025-9.

Sageman, Marc (2004). "Understanding Terror Networks". Philadelphia, PA: University of Pennsylvania Press, ISBN: 0-8122-3808-7.

##### **B. Recommended Supplemental Texts – NOT REQUIRED.**

Gerges, Fawaz A. (2007). "Journey of the Jihadist: Inside Muslim Militancy". New York: Harcourt Inc., ISBN: 978-0-15-101213-8.

Sloan, Stephen (2006). "Terrorism: The Present Threat in Context". New York: Berg Publishers, ISBN: 978-1-84520-344-3.

##### **C. Readings.**

Required readings, and sometimes additional or substitute readings, will be provided either via e-mail or during classroom sessions. Students are encouraged to read additional homeland security and homeland defense literature beyond the required readings and are encouraged to share relevant articles with the class.

## **V. COURSE OUTLINE.**

### **Lesson 1 - Introductions**

- Course Syllabus / Class Contact Roster / Introductions / Intro to Course
- Handout:
  - *Strategic Counter-Terrorism: Getting Ahead of Terrorism; Part 1: Understanding the Threat*
- Videos:
  - Walid Shoebat
  - Obsession

### **Lesson 2 - Understanding Jihad**

- Marc Sageman: Ch. 1 & 2
- Handouts:
  - *Al-Suri's Doctrines for Decentralized Jihadi Training - Part 1*
  - *Al-Suri's Doctrines for Decentralized Jihadi Training - Part 2*

### **Lesson 3 - Mindset and Methods of a Terrorist**

- Mike German: Ch. 5 - 10
- Handouts:
  - *Knowing the Enemy*
  - *The Threat of Grassroots Jihadi Networks: A Case Study from Ceuta, Spain*
- Assignment Due: First Issue Paper

### **Lesson 4 - Domestic Terrorism and Extremist Groups**

- Mike German: Ch. 11 - 12
- Handout:
  - *Guerilla Warfare and Law Enforcement*

### **Lesson 5 - Domestic Terrorism, Organized Crime, Gangs, and al-Qaeda**

- Steve Emerson: Ch. 11
- Handouts:
  - *Gangs: A Threat to National Security*
  - *Mara Salvatrucha: The New Face of Organized Crime?*
  - *The Most Dangerous Gang in America*

### **Lesson 6 - Jihad Recruiting and al-Qaeda Network**

- Steve Emerson: Ch. 3 & 12
- Handouts:
  - *Khalid Sheikh Muhammad: Waging Jihad from Prison*

- *Online Islamists Attempt to Recruit Fighters for the Somali Jihad*
- *Al-Qaeda's Caucasian Foot Soldiers*
- Videos:
  - American al-Qaeda
  - Al-Qaeda Training Camp
- Assignment Due: Domestic Terrorist Group Paper

### **Lesson 7 - Hamas "Harakat Al-Muqawama Al-Islamia"**

- Steve Emerson: Ch. 5
- Handouts:
  - *Fatah and Hamas: The New Palestinian Factional Group*
  - *Hamas Accused of Caving In to International Pressure*
  - *The Sunni Islamists' Changing Reform: What Hamas really wants*
- Video:
  - Hamas

### **Lesson 8 - Hizballah "The Party of God"**

- Steve Emerson: Ch. 6
- Video:
  - Hizballah
- Assignment Due: Second Issue Paper

### **Lesson 9 - Palestinian Islamic Jihad**

- Steve Emerson: Ch. 7

### **Lesson 10 - Pakistani Jihadist Network**

- Steve Emerson: Ch. 8
- Handouts:
  - *The Pakistan-Jihadist Connection*
  - *The Network*

### **Lesson 12 - Charities, Foundations, and Financing**

- Steve Emerson: Ch. 9
- Handouts:
  - *Wanting to Stay Sealed*
  - *Perilous Power Play*
- Assignment Due: Third Issue Paper

### **Lesson 13 - Social Networks**

- Marc Sageman: Ch. 5
- Handouts:

- *The Ideological Voices of the Jihadi Movement*
- *The New Issue of Technical Mujahid, a Training Manual for Jihadis*

#### **Lesson 14 - The SAAR Network**

- Steve Emerson: Ch. 10
- Handouts:
  - *Wanting to Stay Sealed*
  - *Perilous Power Play*
- Assignment Due: International Terrorist Group Paper

#### **Lesson 15 - Female Homicide Bombers**

- PowerPoint Presentation
- Handouts:
  - *Female Shiite Assassination Groups Dispatched to Baghdad*
  - *My dream was to be a suicide bomber*
  - *Hamas prefers "bad girls" to be bombers*
  - *Al-Aksa announce female bomber unit*
  - *Muslim Female Fighters: An Emerging Trend*
  - *Profile of a Female Suicide Bomber*
- Video:
  - *Palestinian Terrorist Woman*