**Course Number: XXXXXX**

**Course: Critical Infrastructure Security and Resilience: Methods, Policies, and Strategies**

**University of XXXXXX**

**Fall/Spring Semester 20XX**

**Name of School:**

**Department:**

**Program:**

**Professor:**

Telephone Number:

Office Location:

Office Hours:

Email:

Website:

**Course Description/Overview:**

This course facilitates student-centered learning, integrates critical decision-making, and uses historical event case studies to reinforce national security and homeland security policies governing the security, identification, and resilience of the nation’s critical infrastructure from an all-hazards context with emphasis on the prevention, mitigation, and response to adversary attack scenarios against single or multiple critical infrastructure sectors.

**Credits Conferred: 3**

**prerequisite:** Introduction to Critical Infrastructure Security and Resilience

In addition to successfully completing Introduction to Critical Infrastructure Security and Resilience, each learner is expected to perform graduate-level work, understand basic management principles, and be able to apply appropriate knowledge and techniques to real-world situations. Learners should have the ability to conduct research, compile a list of appropriate sources, analyze the data, and draw conclusions based on that research.

**Learner Outcomes/Objectives (As mapped against Department of Homeland Security Critical Infrastructure Core Competencies):**

**Learner Outcomes:** This course is designed to enable learners to:

1. Identify key national security policy shifts and the competition between security, freedom, and privacy since 9/11 that has impacted the definition of critical infrastructure.
2. Examine the roles and responsibilities of the U.S. National Security and Homeland Security Councils in the development, implementation, and management of national strategies for homeland defense and security.
3. Identify the roles and responsibilities of government, private sector, and non-government organizations (NGO) to protect critical infrastructure systems.
4. Analyze key elements needed in an effective physical and cybersecurity protection system and the integration of science and technology to counter and mitigate asymmetric and advanced persistent threats.
5. Understand the need for a dynamic methodology in the prevention, mitigation, and response to an all-hazards approach and continuity of government.

**Learning Objectives:** This course is designed to prepare learners to:

**1.** Discuss the rationale for establishing the Department of Homeland Security (DHS), identifying critical infrastructure systems, and publishing Homeland Security Presidential Directives (HSPD).

**2.** Analyze the national security strategy released by the White House in May 2010 that lays out a strategic approach to secure the nation against 21st-century threats.

**3.** Develop a working knowledge through the use of case studies of what constitutes critical infrastructure and resilience in preventing, mitigating, and responding to malevolent acts and natural disasters.

**4.** Defend the need for clear and unambiguous concepts when defining risk terms and risk methodologies used to protect critical infrastructure and to assess the resilience of these assets.

**5.** Construct all-hazards and attack scenarios against critical infrastructure based on postulated threats and historical examples and identify possible effective countermeasures.

1. Assess the resilience of a given critical infrastructure sector(s), network, or function.

**7.** Discuss the impact of three supply-chain issues on any two critical infrastructure sectors during a major incident.

**Delivery method:**

This course features seminar-style discussions — stimulated by lectures and case studies focused on course goals — and learning objectives, both supplemented by current international and national critical infrastructure and resilience all-hazards and security issues selected from the news media and the DHS Blog (http://www.dhs.gov/blog ). Learners will have the opportunity to lead class discussions and to make presentations to enhance the learning process.

The assigned course reading include a variety of resources, such as authoritative readings (legislation, executive orders, policies, plans and strategies), implementation readings (government products that are responsive or attempt to fulfill the requirements of authoritative documents), and external reviews (U.S. Government Accountability Office, Congressional Research Service, etc.). Learners are expected to familiarize themselves with the assigned topic and readings before class and should be prepared to discuss and debate them critically as well as analyze them for biases and multiple perspectives.

**General Course Requirements:**

1. Class attendance is both important and required. If, due to an emergency, you will not be in class, you must contact your instructor via phone or email. Learners with more than two absences may drop a letter grade or lose course credit.
2. It is expected that assignments will be completed on time (the beginning of the class in which they are due). However, it is recognized that learners occasionally have serious problems that prevent work completion. If such a dilemma arises, please speak to the instructor in a timely fashion.
3. The completion of all readings assigned for the course is assumed. Because the class will be structured around discussion and small group activities, it is critical for you to keep up with the readings and to participate in class.
4. Follow university policy regarding use of electronic devices while class is in session.

**Grading/Course requirements:**

The three basic requirements for the course are worth a total of 100 points:

1. **Participation:** This will be based on class attendance, completion of assignments, active participation in case studies, and informed contribution to class discussions.
2. **Group Case Studies**: Examining historical events using a case study methodology will facilitate key teaching points and critical infrastructure lessons learned. The case study format is located at the end of this syllabus.
3. **Term Paper:** Completion of a 15-20 page term paper, and in-class presentation of a summary of findings.

Class Participation 20%

Group Case Study 20%

Presentations 20%

Term Paper 40%

**Activities, Exercise, and Research Projects:**

**1.** Prepare attack and all-hazards scenarios targeting critical infrastructure systems to identify adversary attack scenarios, all-hazards risks, and evaluate countermeasures and resilience.

**2.** Present group case studies that identify critical infrastructure issues based on a contemporary historical event included in the list at the end of this syllabus.

**3.** Write a term paper on a critical infrastructure security and resilience topic approved by the instructor and conduct a presentation to the class. Term paper presentations are scheduled for the last two classes.

**incorporation of feedback:**

The course instructor will offer multiple opportunities for learners to provide constructive feedback over the period of the course. These feedback channels may take the form of group sessions or one-on-one sessions with the instructor. Learners will be afforded the opportunity to complete in-class evaluations at the end of Lesson 6, following the first of the two scheduled critical-infrastructure incident-management case studies, and at the end of the course. Online feedback is also encouraged throughout the course. The instructor will provide written feedback on case studies and term papers. Ongoing dialogue with the instructor regarding term papers and case study preparation is highly encouraged.

**Course Readings:**

The primary textbook will be supplemented by additional readings accessible at website addresses provided in the syllabus.

**Course Textbooks:**

Mary Lynn Garcia, *The* *Design and Evaluation of Physical Protection Systems*, 2nd ed., (Butterworth-Heinemann, 2008).

**Articles and Reports:**

*The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* Official Government Edition, (GPO, 2004), Chapters 2, 3, 6, 7, 10, and 11,

<http://www.gpoaccess.gov/911/>.

*National Security Strategy,* May 2010,
<http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

*National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, December 2013,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

*The National Strategy to Secure Cyberspace,* February 2003,

<http://www.us-cert.gov/security-publications/national-strategy-secure-cyberspace>.

*Department of Homeland Security Strategic Plan Fiscal Years 2012–2016,* February 2012,<http://www.dhs.gov/strategic-plan-fiscal-years-fy-2012-2016>.

*DHS Risk Lexicon 2010 Edition,*<http://www.dhs.gov/files/publications/gc_1232717001850.shtm>.

*The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets,* February 2003,

<http://www.dhs.gov/files/publications/publication_0017.shtm>.

*Homeland Security Presidential Directive 7— Critical Infrastructure Identification, Prioritization, and Protection,* December 2003,<http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1>.

*Presidential Policy Directive-21*, *Critical Infrastructure Security and Resilience*, February 2013,

<http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

**Websites:**

*Critical Infrastructure Sectors*,
<http://www.dhs.gov/critical-infrastructure-sectors>.

*Critical Infrastructure Security,*

<http://www.dhs.gov/files/programs/critical.shtm>.

*Homeland Security Presidential Directives,*<https://www.hsdl.org/?collection&id=2481>.

*The National CI/KR Protection Annual Report*,

<http://www.dhs.gov/xlibrary/assets/nipp_annrpt.pdf>.

*George Mason University Center for Infrastructure Protection and Homeland Security,* <http://cip.gmu.edu/>.

*The CIP Report,*

<http://cip.gmu.edu/the-cip-report/>.

*International Issues for CI/KR Protection,* <http://www.dhs.gov/xlibrary/assets/nipp_international.pdf>.

U.S. Fire Administration (FEMA)*, Critical Infrastructure Protection,*

<http://www.usfa.fema.gov/fireservice/emr-isac/index.shtm>.

*National Infrastructure Protection Plan Sector Partnership Model,*

<http://www.dhs.gov/xlibrary/assets/NIPP_SectorPartnership.pdf>.

Critical Infrastructure and Key Resources Sector Partnership Ethics Guidelines*,* follow *Standards of Ethical Conduct for Employees of the Executive Branch*, (current as of July 1, 2014),

<http://www.ecfr.gov/cgi-bin/text-idx?SID=2d8613038a03bc8e0299ba1c84f87515&node=5:3.0.10.10.9&rgn=div5>.

Department of Homeland Security, *Science and Technology Directorate Technology Clearinghouse / R-Tech*

<http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm>.

**Reference Textbooks:**

Betty E. Biringer, Rudolph V. Matalucci, and Sharon O'Connor, *Security Risk Assessment and Management: A Professional Practical Guide for Protecting Buildings and Infrastructure*, (John Wiley and Sons, 2007).

Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,* (The National Academies Press, 2002),

<http://books.nap.edu/catalog.php?record_id=10415>.

Albert-László Barabási, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life*, (Basic Books, 2014).

Joshua Cooper Ramo, [*The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us And What We Can Do About It*](http://www.amazon.com/Age-Unthinkable-Disorder-Constantly-Surprises/dp/0316118117/ref%3Dsr_1_1?s=books&ie=UTF8&qid=1279836402&sr=1-1), (Little, Brown and Company – 2010).

**Grading Scale (School Policy Dependent):**

**Course Topics:**

|  |  |
| --- | --- |
| **Lesson** | **Topic and Case Studies\*** |
| Lesson 1 | Overview of National Security and Department of Homeland Security Frameworks |
| Lesson 2 | Critical Infrastructure Security and Resilience  |
| Lesson 3 | Critical Infrastructure Security and Resilience: Sector-Specific Plans |
| Lesson 4  | Natural Disasters, Threats, Attack Scenarios, and Countermeasures  |
| *Case Study* | *Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments* |
| Lesson 5  | Threats, Attack Scenarios, and Countermeasures |
| *Case Study* | *Mumbai Attacks, 2008* |
| Lesson 6 | Intelligence, Counterintelligence, and Information Sharing  |
| Lesson 7 | Design and Evaluation of Protection Systems  |
| Lesson 8 | Design and Evaluation of Protection Systems |
| *Case Study* | *Fort Hood Shootings, 2009* |
| Lesson 9 | Protect and Maintain Telecommunications and Information Technology |
| *Case Study* | *Internet Attacks, 2011* |
| Lesson 10 | International Critical Infrastructure Systems and Dependency |
| Lesson 11 | Science and Technology  |
| Lesson 12 | Future Challenges to Critical Infrastructure  |
| Lesson 13 | Future Challenges to Critical Infrastructure  |
| *Case Study* | *Japan’s Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy* |
| Lesson 14 | Student Term Paper Presentations |
| Lesson 15 | Student Term Paper Presentations |
| \*Student-Group Case Study Presentations will be from open sources only |

**Course Outline**

**Lesson 1**: **Overview of National Security and Department of Homeland Security Frameworks**

**1. Lesson Goals/Objectives:**

* Define course requirements and expectations
* Differentiate between national defense and homeland security and understand how they complement one another
* Identify key national security strategies in protecting the homeland
* Contrast pre- and post-9/11 national security issues
* Examine the current organizational structure of DHS
* Identify four issues in the article *The Response of People to Terrorism* that should be of concern to the critical infrastructure community

**2. Discussion Topics:**

* How do the terms “national security” and “homeland security” differ?
* Identify key national security strategies for the protection of critical infrastructure and enhancing its resilience.
* How many critical infrastructure sectors are interdependent?
* What role should science and technology have in countering terrorism?
* What are the implications of “countering terrorism” versus preparing for “all-hazards?”

**3. Required Reading:**

*National Security Strategy,* May 2010, [review only]
<http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf>.

*NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, December 2013,

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

*Critical Infrastructure Security,*

<http://www.dhs.gov/files/programs/critical.shtm>.

President’s Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America’s Infrastructures*, October 1997,

[*http://www.fas.org/sgp/library/pccip.pdf*](http://www.fas.org/sgp/library/pccip.pdf).

Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,* (The National Academies Press, 2002), Chapter 9: “The Response of People to Terrorism,”

<http://books.nap.edu/catalog.php?record_id=10415>.

1. **Activities:**
* Small discussion groups will identify five pre- and five post-9/11 critical infrastructures issues and present their findings to the class.
* DVD: *The World Trade Center (WTD): The First 24 Hours*

**Lessons 2 & 3: Critical Infrastructure Security and Resilience; Sector-Specific Plans**

**1. Lesson Goals/Objectives:**

* Evaluate how the definition of terrorism shapes U.S. policy toward critical infrastructure
* Define the terms “critical infrastructure security” and “resilience”
* Describe the national strategies for protecting the critical infrastructure
* Highlight the differences between vulnerability, threat, consequence, and risk assessment
* Explain the issues in policy implementation to protect the critical infrastructure
* Define the differences in protection and resilience strategies between a fixed and mobile critical infrastructure system
* Identify the role of the National Response Framework (NRF) in critical infrastructure prevention, impact mitigation, and emergency response

**2. Discussion Topics:**

* Identify four issues in the article *The Response of People to Terrorism* that should be of concern to the critical infrastructure community.
* Evaluate key considerations between the protection strategies for fixed and mobile infrastructure assets.
* What are the principal challenges faced in protecting the nation’s critical infrastructure?
* What level of interdependency exists for each critical infrastructure sector?
* Analyze three issues of concern with complex and interdependent critical infrastructure systems and sectors.
* Define the importance of critical infrastructure resilience.
* Explain the role science and technology should play in prevention, mitigation, and response to critical infrastructure systems.

**3. Required Reading:**

Mary Lynn Garcia, *The* *Design and Evaluation of Physical Protection Systems*, 2nd ed., (Butterworth-Heinemann, 2008), Chapter 15: “Risk Assessment.”

*The 9/11 Commission Report,* Chapter 2,

<http://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT-8.pdf>.

*The National Strategy for The Physical Protection of Critical Infrastructures and Key Assets,* February 2003,

<http://www.dhs.gov/files/publications/publication_0017.shtm>.

*National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience*, December 2013, [review only].

<http://www.dhs.gov/sites/default/files/publications/NIPP%202013_Partnering%20for%20Critical%20Infrastructure%20Security%20and%20Resilience_508_0.pdf>.

Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism,* (The National Academies Press, 2002),

<http://books.nap.edu/catalog.php?record_id=10415>.

* Chapter 8: City and Fixed Infrastructure
* Chapter 10: Complex and Interdependent Systems

*National Response Framework (NRF)*, 2nd Edition, May 2013.

<http://www.fema.gov/media-library-data/20130726-1914-25045-1246/final_national_response_framework_20130501.pdf> [review only].

American National Standards Institute, *Organizational Resilience: Security, Preparedness, and Continuity Management Systems—Requirements with Guidance for Use*, ASIS SPC.1-2009, (ASIS International, 2009),

<https://www.asisonline.org/Standards-Guidelines/Standards/Pages/Resilience-Standards.aspx> (free download only for ASIS members)

<http://www.ndsu.edu/fileadmin/emgt/ASIS_SPC.1-2009_Item_No._1842.pdf>

National Infrastructure Advisory Council, *Critical Infrastructure Resilience Final Report and Recommendations*, September 2009, [review only], <http://www.dhs.gov/xlibrary/assets/niac/niac_critical_infrastructure_resilience.pdf>.

*National Infrastructure Protection Plan Sector-Specific Plans,* [review only]

<http://www.dhs.gov/xlibrary/assets/nipp_sctrplans.pdf>.

<http://www.dhs.gov/critical-infrastructure-sectors>. [click on each sector for a link to each SSP]

**4. Activity:**

* Learners will navigate the DHS website responding to questions from the instructor concerning the location of specific topics.

**Lesson 4: Natural Disasters, Threats, Attack Scenarios, and Countermeasures**

**1*.* Learning Goals/Objectives:**

* Contrast how prevention, mitigation, and response differ between a natural and man-made threat
* Define the term “threat shifting” as used in the *2010 DHS Risk Lexicon*
* Explain why the conduct and use of a risk assessment by government and industry may differ

**2. Discussion Topics:**

* The term “threat” is used in many different contexts. Analyze the meaning of “threat” as it applies to an all-hazards approach.
* Should unintentional industrial accidents be considered threats under an all-hazards approach?
* What are the similarities between a natural and man-made threat?
* What is the meaning of the term “technological threat”?
* How are consequences determined when evaluating a natural disaster and man-made event?
* How does “new terrorism” differ from terrorism previous to the 9/11 attacks?
* Explain how and why terrorism tactics, techniques, and procedures are continually evolving? What impact does this have on preventing, mitigating, and responding to attack scenarios?

**3. Required Reading:**

*The 9/11 Commission Report*

* Chapter 2: The Foundation of the New Terrorism
* Chapter 3: Counterterrorism Evolves
* Chapter 6: From Threat to Threat
* Chapter 7: The Attack Looms

**4. Activity:**

* Presentation of case study
* *Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments*

**Lesson 5: Threats, Attack Scenarios, and Countermeasures**

**1. Learning Goals/Objectives:**

* Highlight the differences between a vulnerability and risk assessment
* Explain how critical assets, threats, and consequences are used to evaluate risk
* Define how risk is managed
* Identify the three physical protection functions
* Compare the different types of countermeasures

**2. Discussion Topics:**

* Does a facility characterization include supporting missions?
* How would you define countermeasures?
* How does the threat drive the establishment of countermeasures?
* From whose perspective is target identification addressed? How are targets selected (e.g., what criteria are used and why)?
* What key elements are evaluated during the analysis and evaluation phase of the design and evaluation of physical protection?
* In addition to the physical protection systems, what other systemic issues must be considered?
* Threat shifting is the response of adversaries to perceived countermeasures or obstructions in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle (DHS Risk Lexicon, 2010, p. 37). How does threat shifting increase or decrease risk?

**3. Required Reading:**

Mary Lynn Garcia. *The* *Design and Evaluation of Physical Protection Systems*, 2nd ed., (Butterworth-Heinemann, 2008).

* Chapter 2: Facility Characterization
* Chapter 3: Threat Definition
* Chapter 4: Target Identification
* Chapter 13: Analysis and Evaluation

National Terrorism Advisory System (NTAS) [review only],

<http://www.dhs.gov/national-terrorism-advisory-system>

**4. Activity:**

* Case Study
* *Mumbai Attacks, 2008*

Note: A balanced approach is critical to identify effective countermeasures based on level and severity of natural and man-made threats (e.g., all hazards) along with a detailed site characterization that provides senior management with decision options. Politics from many levels will influence the risk assessment process.

**Lesson 6: Intelligence, Counterintelligence, and Information Sharing**

**1. Learning Goals/Objectives:**

* Identify members of the national intelligence and information sharing communities
* Explain the difference between information and intelligence
* Define the role of the intelligence community in supporting DHS
* Identify how community involvement is related to countering threats against critical infrastructure systems
* Identify how the DHS Office of Operations Coordination and Planning can deter, detect, and prevent terrorist acts and facilitate effective response to other incidents
* Explain the term “information sharing” as it pertains to the 16 sectors
* Define “Safeguard New York”

**2. Discussion Topics:**

* How should the community become involved in protecting critical infrastructure?
* Describe information-sharing partnerships with the private sector. What barriers are there to sharing information?
* By what criteria does a private business base its decision to become involved with an information-sharing relationship with the public sector?
* Information sharing is a key element of our national strategy in counterterrorism and homeland security. What are the pros and cons of information sharing?
* The Nationwide Suspicious Activity Report (SAR) Initiative (NSI) was established to provide a unified process for reporting, tracking, and accessing information that may forewarn of a future terrorist attack. The long-term goal is for Federal, State, local, tribal, and territorial law enforcement organizations, as well as private sector entities, to participate in the National SAR initiative. What type of information is needed from SAR to protect critical infrastructure sectors?
* How does Safeguard New York apply to the critical infrastructure sectors?

**3. Required Reading:**

Office of the Director of National Intelligence (ODNI) [review only],<http://www.dni.gov/>.

Office of the Director of National Intelligence, *ODNI FAQ*,
<http://www.dni.gov/index.php/about/faq>.

U.S. Department of Homeland Security, *Counterterrorism Publications* [review the “Protecting, Analyzing & Sharing Information” section],

<http://www.dhs.gov/counterterrorism-publications>.

*United States Intelligence Community Information Sharing Strategy*, February 2008,
<http://www.fas.org/irp/dni/iss.pdf>.

*The CIP Report*, May 2010, “Information Sharing”,

<http://tuscany.gmu.edu/centers/cip/cip.gmu.edu/wp-content/uploads/2013/06/CIPHS_TheCIPReport_May2010_InformationSharing.pdf>.

National Suspicious Activity Reporting (SAR) Initiative (NSI),

 <http://nsi.ncirc.gov/>.

Public Transportation Sector Information Sharing,

<http://www.apta.com/resources/safetyandsecurity/Pages/ISAC.aspx>.

Sharing with the Private Sector,

<http://www.ise.gov/sharing-private-sector>.

DHS *Office of Operations Coordination and Planning*,

<http://www.dhs.gov/about-office-operations-coordination-and-planning>.

*Safeguard New York*,

<http://www.dhses.ny.gov/oct/safeguardNY/>

Note: Not all customers or agencies use the same criteria for defining classification categories or levels of sensitivity. Consult Federal, State, local, tribal, and territorial guidance for classified and other sensitive official materials.

**Lessons 7 & 8: Design and Evaluation of Protection Systems**

**1. Learning Goals/Objectives:**

* Evaluate the necessary elements of a physical protection system
* Explain how response is integrated into the protection of critical infrastructure
* Create a countermeasure plan, given a schematic of a critical infrastructure asset
* Discuss the role of private security in infrastructure protection

**2. Discussion Topics:**

* Physical protection technology and hardware are elements of a robust physical protection system. What other elements are required to have an integrated physical protection system?
* A key element in designing and implementing a physical protection system is senior management buy-in. In the private sector, the bottom-line is always profitability and return-on-investment. How would you persuade senior management that a new or upgraded physical protection system is cost effective?
* Numerous vendors provide physical security systems, some reputable and some not so reputable. When evaluating the purchase of or upgrading to a physical protection system, what criteria should be used in evaluating the trustworthiness of a vendor?
* Postulated threats are used while planning to prevent, mitigate, and respond to hypothetical scenarios. What mechanisms are necessary to maintain updated information on emerging threats?
* A common threat scenario is for an adversary to be disguised as a legitimate vendor. What policies and procedures would you need in place to verify a vendor’s identity?
* Exterior and interior intrusion security protection systems are used to provide defense-in-depth and detection. Describe the criteria used in the decision process for selecting an exterior or interior system.

**3. Required Reading:**

Mary Lynn Garcia. *The* *Design and Evaluation of Physical Protection Systems*, 2nd ed., (Butterworth-Heinemann, 2008).

* Chapter 1: Design and Evaluation of Physical Protection Systems
* Chapter 5: Physical Protection System Design
* Chapter 6: Exterior Intrusion Sensors
* Chapter 7: Interior Intrusion Sensors
* Chapter 10: Entry Control

 **4. Activities:**

* Create a countermeasure plan
* Case Study:
* *Fort Hood Shootings, 2009*

Note: The majority of critical infrastructure is owned or operated by the private sector.

Each site’s unique risk assessment and component-systems integration (e.g., contract security, proprietary security, law enforcement, emergency management, Federal, State, local, tribal, and territorial resources) must be considered in an overall security and resilience strategy—prevention, protection, mitigation, response, and recovery.

**Lesson 9: Secure and Maintain Telecommunications and Information Technology**

**1. Learning Objectives:**

* Define cybersecurity, cybercrime, and cyber-terrorism
* List critical infrastructure cyber vulnerabilities
* Evaluate the emerging advanced persistent cyber threat against critical infrastructure
* Identify the strategic goal of DHS in combating cyber threats
* Understand the potential effectiveness of a combined cyber and physical attack against critical infrastructure

**2. Discussion Topics:**

* Explain why the cyber threat is a seminal issue in securing critical infrastructure systems.
* One expert believes “The convergence of technological and socio-political trends indeed suggests that cyber-terrorism may be the wave of the future” (Andrew Rathmell,“*Cyber-terrorism The Threat of the Future*?”, RUSI Journal, vol. 142, no. 5, October 1997, reprinted by Rand Corporation in 2003.). Assuming this is a true statement, what are the strategic implications in the protection and resilience of critical infrastructure?
* The *National Strategy to Secure Cyberspace* provides a framework for protecting the infrastructure. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, and most recently by Executive Order 13636*, Improving Critical Infrastructure Cybersecurity*. Explain the relationship between these documents. Do they provide a sufficient response to the cyber threat?
* The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. The private sector is hesitant to report such attacks. Why is this? What can be done to increase reporting?
* A key ingredient of the Advanced Persistent Threat (APT) is the abuse and compromise of “trusted connections.” What does this mean? How can this threat be countered?

**3. Required Reading:**

*Department of Homeland Security Strategic Plan Fiscal Years 2012–2016,* February 2012,<http://www.dhs.gov/strategic-plan-fiscal-years-fy-2012-2016>.

*The National Strategy to Secure Cyberspace,* February 2003, [review only]

<http://www.us-cert.gov/security-publications/national-strategy-secure-cyberspace>.

Executive Order 13636, Improving Critical Infrastructure Cybersecurity, 2013. <http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

DHS *Office of Cybersecurity and Communications*, [review only],

<http://www.dhs.gov/office-cybersecurity-and-communications>.

*Statement of General Victor E. Renuart, Jr. USAF, Commander, United States Northern Command and North American Aerospace Defense Command, Before the Senate Armed Services Service Committee*, 11 March 2010, <http://www.rand.org/content/dam/rand/www/external/nsrd/DoD-CBRNE-Panel/panel/meetings/20100317/D-4-Statement-of-Commander-United-States-Northern-Command.pdf>.

*Cyberspace Policy Review*, 2009, <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

*Advanced Persistent Threats* (APTs),

<http://www.damballa.com/knowledge/advanced-persistent-threats.php>.

**4. Activity:**

* Case Study:
* *Internet Attacks, 2011*

Robert Johnson, “The Biggest Hacking Attacks Of 2011,” *Business Insider*, June 13, 2011,

<http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-6?op=1>.

**Lesson 10: International Critical Infrastructure Systems and Dependency**

**1. Learning Objectives:**

* Discuss national and international security implications where critical infrastructure shares international boundaries
* Identify critical infrastructure sectors that cross the U.S. borders with Canada and Mexico
* Compare national and international issues in critical infrastructure
* Assess the complexity and interdependency of critical infrastructure in a global economy

**2. Discussion Topics:**

* What are U.S. critical infrastructure security implications from countries that do not share our borders?
	+ Identify possible disruption of manufacturing and supply?
	+ What are the pros and cons in information sharing?
	+ What can we learn from these countries?
* As globalization, internationalism, environmental concerns (e.g., global warming), and limited resources become more pronounced in the 21st century, how will these factors play out in protecting our nation’s critical infrastructure?
* The world is becoming more complex and interdependent. New technologies are emerging, boundaries are disappearing, and social media is used to topple governments. The internet has changed economics, culture, and politics. As these changes accelerate, what impact will they have on national and international critical infrastructure systems?

**3. Required Reading:**

*International Issues for CI/KR Protection,* <http://www.dhs.gov/xlibrary/assets/nipp_international.pdf>.

*The CIP Report,* George Mason University Center for Infrastructure Protection and Homeland Security,

<http://cip.gmu.edu/the-cip-report/162-2/>:

* June 2010 International *CIP*

Afghanistan Infrastructure, page 9

Infrastructure Regulation, page 10

* July 2009 International *CIP*

Australian Infrastructure, page 2

Italian Infrastructure Protection, page 5

* June 2008 International *CIP*

Australian Resilience Planning, page 4

European Union CIP, page 9

**4. Activity:**

* Divide learners into groups to identify international interdependencies in critical infrastructure security. Assign a different country to each; group leader presents findings.

**Lesson 11: Science and Technology**

**1. Learning Objectives:**

* Explain how DHS provides knowledge products and innovative technology solutions for homeland security
* Identify the kinds of research DHS is conducting to address critical homeland security needs
* Identify how DHS transitions and commercializes the results of its technology research for use by the critical infrastructure community
* Describe the advantages and disadvantages of technology in critical infrastructure systems

**2. Discussion Topics:**

* Renewed focus on counterterrorism (CT) and homeland security has served as a catalyst to promote the increased use of technology. What are some of the advantages and disadvantages within a democratic society expanding the use of these technologies?
* Where do you see gaps in CT and homeland security capabilities that might be filled by new technology?
* Explain the role science and technology should play in the prevention, mitigation, and response to critical infrastructure incidents.
* Use of the latest security technology is often touted as the "solution." What criteria should be used before investments are made in state-of-the-art security technology?

**3. Required Reading:**

Committee on Science and Technology for Countering Terrorism, National Research Council, *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, (The National Academies Press, 2002), Chapter 10: “Complex and Interdependent Systems.”

*The 9/11 Commission Report*

* Chapter 10: War Time
* Chapter 11: Foresight—And Hindsight

Department of Homeland Security, *Science and Technology Directorate Technology Clearinghouse / R-Tech* [review only],

<http://www.dhs.gov/xfrstresp/training/gc_1174057429200.shtm>.

Lois M. Davis et al., *Long-Term Effects of Law Enforcement’s Post-9/11 Focus on Counterterrorism and Homeland Security Summary Report*, (Rand Corporation, 2010),<http://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG1031.sum.pdf>**Lesson 12 & 13: Future Challenges to Critical Infrastructure**

**1. Learning Objectives:**

* Identify and evaluate emerging natural and man-made threats and their impact on critical infrastructure systems
* Explain how advanced persistent threats (APTs) could impact critical infrastructure systems
* Explain the rationale for continuous improvement of the NIPP and SSPs

**2. Discussion Topics:**

* In July 2010, DHS launched a national "If You See Something, Say Something™" public awareness campaign.
	+ What criteria would you use to evaluate the effectiveness of such a public awareness campaign?
	+ What are some of the advantages and disadvantages of these programs?
	+ Can you identify similar programs in your jurisdiction?
	+ What role does culture play (e.g., Israel vs. U.S.)?
* As new terrorist threats emerge and the adversary adapts seemingly overnight to introduce new attack scenarios (e.g., liquid explosives, selecting unknowing individuals as suicide bombers, secreting explosives in body cavities, etc.), it has become more difficult to neutralize these threats. Most critical infrastructure systems are at fixed physical locations, i.e., hard targets. An emerging trend is to attack mobile or soft targets (e.g., railways, subways, crowds, etc.). As these trends emerge, how flexible do we need to be in order to get ahead of the threat? How would this be accomplished?
* In a democratic society “freedom” and “security” are always at odds because security implies restrictions. Seeking to balance these two competing goals makes for difficult choices. Are individual rights paramount or do the means justify the ends in preventing another 9/11?
	+ What criteria would you use in achieving equilibrium between these two competing goals?
	+ How would you quantify the costs if one goal greatly outweighed the other?
* The *Strategic National Risk Assessment* evaluated events that have a distinct beginning and end and omitted evaluating political, economic, environmental, and societal trends that may contribute to a changing risk environment but are not explicitly homeland security national-level events (e.g., demographic shifts, economic trends, aging infrastructure, climate change). How should governmental and private-sector critical infrastructure leaders prepare for such shifts?

**3. Required Reading:**

*National Prevention Framework,* May 2013,

<http://www.fema.gov/national-prevention-framework>

<http://www.fema.gov/media-library/assets/documents/32196?id=7358>.

*U.S. Counterterrorism Strategy Must Address Ideological and Political Factors at the Global and Local Levels,*<http://www.rand.org/pubs/research_briefs/RB202/index1.html>.

*National Infrastructure Protection Plan Sector-Specific Plans,* [review only]

<http://www.dhs.gov/xlibrary/assets/nipp_sctrplans.pdf>.

<http://www.dhs.gov/critical-infrastructure-sectors>. [click on each sector for a link to each SSP]

Jena Baker McNeill and James Jay Carafano, “Terrorist Watch: 23 Plots Foiled Since 9/11,” *Backgrounder*, (The Heritage Foundation, July 2009),

<http://www.heritage.org/research/reports/2009/07/terrorist-watch-23-plots-foiled-since-9-11> .

Brian Michael Jenkins, *Would-Be Warriors: Incidents of Jihadist Terrorist Radicalization in the United States Since September 11, 2001*, (RAND, 2010),

<http://www.rand.org/pubs/occasional_papers/OP292/>.

Anna Speckhard and Khapta Akhmedova, “Black Widows: The Chechen Female Suicide Terrorists,” in Yoram Schweitzer ed., *Female Suicide Bombers: Dying for Equality?*, (Tel Aviv: Jaffe Center for Strategic Studies, 2006) [review only],<http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?ots591=0C54E3B3-1E9C-BE1E-2C24-A6A8C7060233&lng=en&id=91164>.

DHS *"If You See Something, Say Something™" Campaign,*

[http://www.dhs.gov/if-you-see-something-say-something™-campaign](http://www.dhs.gov/if-you-see-something-say-something%E2%84%A2-campaign)

*The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*, December 2011, [review only]

<http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>

*President Obama’s Climate Action Plan Progress Report: Cutting Carbon Pollution, Protecting American Communities, and Leading Internationally*, June 2014,

<http://www.whitehouse.gov/sites/default/files/docs/cap_progress_report_update_062514_final.pdf>.

*Failure To Act: The Impact of Current Infrastructure Investment on America’s Economic Future*, American Society of Civil Engineers, January 2013,

<http://www.asce.org/uploadedFiles/Infrastructure/Failure_to_Act/Failure_to_Act_Report.pdf>.

National Infrastructure Advisory Council, Convergence of Physical and Cyber Technologies and Related Security Management Challenges, 2007,

<http://www.dhs.gov/xlibrary/assets/niac/niac_physicalcyberreport-011607.pdf>.

 **4. Recommended Reading:**
Albert-László Barabási, *Linked: How Everything Is Connected to Everything Else and What It Means for Business, Science, and Everyday Life*, (Basic Books, 2014).

**5. Activity:**

* Case Study:
* *Japan’s Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy*

**Week 14 & 15: Student Term Paper Presentations**

**1. Learning Objectives:**

* Assess how well presenters met the learner outcomes and objectives

**2. Discussion Topics:**

* Term Paper Presentation

**3. Activity:**

* Learners will present a fifteen-minute overview of their term paper
* Each presenter will be prepared to answer relevant questions on their term paper
* Instructor will provide constructive feedback to each presenter

**Case Study Guidance**

**1. Purpose:** Real-world events provide a rich learning environment. Case studies from historical events and natural disasters will be used to highlight course learning objectives.

**2. Goal:** To provide a student-centered learning environment where real-world events can be used as a vehicle linking the academic classroom with actual events. Highlighting issues where policy, procedures, and classroom solutions may not have considered the dynamic and multi-faceted issues confronting critical infrastructure from malevolent and natural disasters, possibly across sectors and international implications.

**3. Action:**

* Small collaborative groups will be assigned a topic to research, write a report, and present findings to the class. The pool of topics include:
* *Hurricane Katrina, 2005-Challenges: Infrastructure and Assessments*
* *Mumbai Attacks, 2008*
* *Fort Hood Shootings, 2009*
* *Internet Attacks, 2011*
* *Japan’s Catastrophic Disaster: Earthquake, Tsunami, and Nuclear Energy*
* *Hurricane Sandy, 2012*
* *Boston Marathon Bombing, 2013*
* Research will be conducted on the assigned topic. ONLY open sources will be used.
* Presentation dates coincide with the lessons listed in **Course Topics** of this syllabus.
* Each group will have thirty minutes to present their report.
* The group will lead a seminar discussion on the topic.
* Each group will provide an electronic copy of slide notes to each student two days prior to the presentation.

**4. References:**

*National Response Framework, Second Edition*, May 2013,

<http://www.fema.gov/national-response-framework>.

*National Preparedness Goal*,

<http://www.fema.gov/national-preparedness-goal>

Review sector-specific plans: [click on relevant sector for a link to each SSP]

<http://www.dhs.gov/critical-infrastructure-sectors>.

*The Strategic National Risk Assessment in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation*, December 2011, [review only]

<http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf>.

**5. Focus:**

* Provide an overview of the assigned case study; identify sector(s) involved and issues related to critical infrastructure resilience based on course learning objectives.
* Additional guidance will be provided during the first class.