EDMG600

Course Summary

Course : EDMG600 **Title :** Emergency Management Perspectives on Cybersecurity
Length of Course : 8
Prerequisites : N/A **Credit Hours :** 3

Description

Course Description: A healthy cyberinfrastructure is the foundation of emergency and disaster management. It provides emergency and disaster management agencies the ability to effectively address and respond to natural disasters, terrorist attacks, and law enforcement issues. Technology has leveled the global playing field, and the impact on the cyberinfrastructure must be assessed among all relevant communities. This means implementing cybersecurity awareness into all levels of emergency and disaster management through: knowledge management, task behavior, dissemination of information, cyberinfrastructure impact awareness, communication, and deterrence. Students will be exposed to planning, management, response, and recovery factors related to cyberinfrastructure, as well as analyze economic, social, and technical aspects of cybersecurity associated with public emergencies and disasters.

Course Scope:

Course covers a broad range of cyber-security, critical infrastructure protection and emergency management concepts, policies, regulations and practices necessary to structure, forecast, recommend, monitor and evaluate cybersecurity problems and challenges from emergency management perspective. Necessary condition for effective intelligence, knowledge acquisition and knowledge management, is a thorough understanding of cybersecurity concepts, issues and challenges. Therefore, significant reading on cybersecurity covers the first half of the course session. Last course module covers global cybersecurity issues and their impact on the U.S. cybersecurity and protection of the U.S. critical infrastructure.

Objectives

After successfully completing this course, you will be able to: After completing the course, the student should be able to:

1. Evaluate conceptual foundations and policy-analytical framework of Cybersecurity
2. Appraise U.S. legal, regulatory and policy contexts and applications of Cybersecurity
3. Evaluate cybersecurity threats to the U.S. Critical Infrastructure
4. Assess the cross-impact and interdependence of Emergency Management and Cybersecurity.
5. Appraise cyber situational awareness from a mitigation, preparedness, response, and recovery standpoint.

6. Review and Assess local and state Cybersecurity and Emergency Management issues
7. Evaluate industry-government partnership and its impact on cybersecurity of U.S. critical infrastructure
8. Analyze global cybersecurity context, discourse and dynamics, and its impact on the U.S. Cybersecurity, critical infrastructure and Emergency Management.

Outline

Week 1:

Topic

Cybersecurity foundations, key concepts, issues, contexts, and debates.

Cyber terrorism framework, cyberwar, customary international law of cyberspace, cyberwar and traditional, open source software, information security, nuclear lessons for cybersecurity, dilemmas of state response to cyber attacks.

Learning Objectives

LO-1: Assess intellectual debate about theoretical foundation and policy-analytical framework of Cybersecurity.

LO-2: Evaluate arguments about the nature of cybersecurity threats
LO-3: Evaluate policy-analytical framework of cybersecurity

Readings

Choose and read *three* articles from the list below:

- Kello, L. (2013). **The meaning of the cyber revolution: Perils to theory and statecraft.** *International Security,* Fall 2013.
- Gartzke, E. (2013). **The myth of cyberwar: Bringing war in cyberspace back down to earth.** *International Security,* Fall 2013.
- Arquilla, J. (2012). **Cyberwar is already upon us.** *Foreign Policy*. March/April, 2012.
- Brown, G. & Poellet, K. (2012). **The Customary International Law of Cyberspace.** *Strategic Studies Quarterly,* 6, no. 3, pp. 126-145.
- Caplan, N. (2013). **Cyber War: the Challenge to National Security**. *Global Security Studies*, Winter 2013, Volume 4, Issue
- Studentnummer, L. van den Boom (2012). **The dilemmas of state response to cyber attacks. Understanding the phenomena, challenges and legal response.** Vrije Universiteit Amsterdam: *Paper Governance of Security and Policing*.
- Crosston, M. D. (2011). **World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence**. *Strategic Studies Quarterly,* 5, no. 1, pp. 100-116.
- Goldsmith, J. (2011). **Cybersecurity Treaties: A Skeptical View. A Future Challenges Essay**. Hoover Institution.
- Mudrinich, E. (2012). **Cyber 3.0: the Department of Defense strategy for operating in cyberspace and the attribution problem.**
- Guinchard, A. (2011). **Between Hype and Understatement: Reassessing Cyber Risks as a Security Strategy.** *Journal of Strategic Security* Volume 4 Number 2 Summer 2011.
- Khosla, P. (2009). **Information Security for the Next Century**. Carnegie Mellon CyLab.
- Hansen, L., & Nissenbaum, H. (2009). **Digital disaster, cyber security, and the Copenhagen School.** *International Studies Quarterly*, 53(4), pp. 1155-1175.
- Kusiak, P. (2012). **Culture, Identity, and Information Technology in the 21st Century: Implications for U.S. National Security**. Carlisle Barracks: U.S. Army War College, Strategic

Studies Institute.
- Libicki, M. C. (2012). **Crisis and Escalation in Cyberspace**. Santa Monica: RAND.
- Nye, J. (2011). **Nuclear lessons for cyber security**. *Strategic Studies Quarterly*. Winter 2011.
- Rid T. (2012). **Think again: Cyberwar**. *Foreign Policy*. March/April, 2012.
- Robinson, N., Gribbon, L., Horvath, V. & Robertson, K. (2013). Cyber-security threat characterization: A rapid comparative analysis. RAND Europe
- Rohan, R. J. (2011). **Social networking, cyberintelligence and cyber counterintelligence**. Utica College.
- Schilling, J. R. (2010). **Defining Our National Cyberspace Boundaries**. Strategy Research Project. Carlisle Barracks: U.S. Army War College.
- Schneider, F. B. & Birman, K.B. (2009). **The monoculture risk put into context**. IEEE *Security & Privacy*.
- Schneider, F. & Mulligan, D. (2011). **Doctrine for cybersecurity**. *Daedalus*. Fall 2011, pp. 70-92.
- Steptoe Cyberblog (2012). **The hackback debate**. Nov. 2, 2012.
- Ahmad, R. & Yunos, Z (2012). **The Application of Mixed Method in Developing a Cyber Terrorism Framework**. *Journal of Information Security*, 2012, 3, pp. 209-214.
- Gourley, B. (2009). **Open Source Software and Cyber Defense.** A White Paper provided to the National Security Council and Homeland Security Council as input to the White House Review of Communications and Information Infrastructure.
- Cote, R. (2011). **The Strategic Paradox of Social Networks. *Strategy Research Project*.** Carlisle Barracks: U.S. Army War College.

Assignment

Week 1 Forum (post under Forums)

- **IMPORTANT ! : Per APUS academic policy and U.S. Department of Education requirements, your introduction must be at least 250 words; Otherwise, you will be dropped from the course.**
- Identify your agency or organization. Identify your job title and duties.
- State your expectations for this course.
- Provide a statement briefly outlining any cybersecurity, intelligence, emergency management, national or homeland security, crisis management, or protective services experiences.
- Give an interesting fact about yourself (e.g., hobby, sport or interest).
- Respond to at least two fellow classmates' introductions.
- **Reflect on your chosen Week 1 reading**:
    - What strikes you as the most persuasive and non-persuasive premise or thesis?
    - Conclude with a research or policy question for further research.

Week 2:

Topic

U.S. Cyberesecurity legal, regulatory and policy context and applications.

Comprehensive National Cybersecurity Initiative, National Strategy for Trusted Identities in Cyberspace, Cyberspace Policy Review Blueprint for a Secure Cyber Future, Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations, International Strategy for Cyberspace, Attribution and Economics, National Security Controls on Science and Technology in a Globalized World.

Learning Objectives

- LO-1: Assess U.S. cybersecurity legal environment
- LO-2: Analyze key U.S. cybersecurity-related regulations
- LO-3: Evaluate US cybersecurity policy context and policy application

Readings

- **Required**: Rollings, J. & Henning, A. C. (2009). **Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations.** Congressional Research Service.
- **Required:** Fischer, E. A. (2012). **Federal Laws Relating to Cybersecurity: Discussion of Proposed Revisions**. Washington, DC: U.S. Library of Congress, Congressional Research Service.
- **Required**: The White House (2011).**The Comprehensive National Cybersecurity Initiative**. Washington, D.C.
- **Required:** The White House (2011). **International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World**. Washington, DC: The White House *(please be patient when downloading. It may take up to five minutes to download the document).*
- **Required**: Department of Homeland Security (2011). **Blueprint for a Secure Cyber Future**.
- Electronic Frontier Foundation, **To the White House Cyber Security Review Team**.
- The White House (2009). **Cyberspace Policy Review**.
- The White House (2011). **National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy**. Washington, D.C.
- Federal Reserve Bank of Dallas (2003). **Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System**.
- United States. Government Accountability Office (GAO) (2011). **Information security: Additional guidance needed to address cloud computing concerns**.
- Internet Security Alliance (2008). **The Cyber Security Social Contract Policy Recommendations for the Obama Administrations and 111th Congress**.
- Owens, W. A., Dam, K. W. & Lin, H. S. (Eds.) (2009). **Technology, policy, law, and ethics regarding U.S. acquisition and use of cyber attack capabilities**. National Research Council. Committee on Offensive Information Warfare. The National Academies Press.
- Committee on Deterring Cyberattacks, National Research Council (2010). **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy**.
- National Research Council (2009). **Beyond 'Fortress America': National Security Controls on Science and Technology in a Globalized World**.
- Brecht, L. A. (2009). **National cyber systems infrastructure security review concept paper**. Capital Markets Research.

Forum

- **Week 2 Forum** (post and discuss under Forums)
  - Respond to the following questions (separate each response with the text of each question):
    1. **What do you believe is the U.S. federal government's weakest and strongest cybersecurity domain/sector/program or concept?**
    2. **How would you reduce weaknesses?**
    3. **How would you design the federal government's cybersecurity management integration across agencies?**
  - **Respond to at least two fellow classmates' posts.**

Week 3:

Topic

Cybersecurity and US Critical Infrastructure Protection.

National Infrastructure Protection Plan; Problems with Extending EINSTEIN 3 to Critical Infrastructure; Cyber Infrastructure Protection; Electricity Grid vulnerabilities; Critical infrastructure information security; and Human Behavior and Insider Attacks.

Learning Objectives

- LO-1: Evaluate cybersecurity threats to the U.S. critical infrastructure
- LO-2: Evaluate FEMA's National Infrastructure Protection Plan
- LO-3: Analyze problems with extending EINSTEIN 3 to Critical Infrastructure

Readings

- ***Required***: Clemente, D. (2013). **Cyber security and global interdependence: What is critical?** Programme Report. February 2013. Chattam House.
- ***Required:*** Bellovin, S. M., Bradner, S. O., Diffie, W, Landau, S. & Rexford, J. (2011). **Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure**. *Harvard National Security Journal*. 3.1, pp. 1-38.
- ***Required***: Saadawi, T & Jordan, J. Jr., (2011). eds. **Cyber Infrastructure Protection**. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute.
- ***Required*****:** FEMA (2013). **National Infrastructure Protection Plan**.
- U.S. Government Accountability Office (2011). **Electricity Grid Modernization: Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to Be Addressed.** Washington, DC.
- Kerfoot, T. (2012). **Cybersecurity: Towards A Strategy for Securing Critical Infrastructure from Cyberattacks**. Silicon Flatirons A Center for Law, Technology, and Entrepreneurship at the University of Colorado.
- Ghosh, C. N. (2000). **EMP Weapons**. Strategic Analysis Volume 24, Issue 7.
- **The potential impacts of three High Power Electromagnetic (HPEM) threats on Smart Grids**. *Electromagnetic Compatibility Magazine*, IEEE, Volume 1, Issue, 2, July 2012.
- Kramer, D. (2009). **US electricity grid still vulnerable to electromagnetic pulses**". *Physics Today*, 62(9), 24..
- **Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack**
- Cowan, E. & Deakin, W. (2008). **Visualisation of critical Infrastructure Failure**. Proceedings of the 9th Australian Information Warfare and Security Conference.Jabbour, K., & Muccio, S. (2011). **The Science of Mission Assurance**. *Journal of Strategic Security*, Volume 4 Number 2.
- Amin, S., Litrico, X., Sastry, S. S., & Bayen, A. M. (2010). **Stealthy deception attacks on water SCADA systems**. Paper presented at the Proceedings of the 13th ACM international conference on Hybrid systems: computation and control.
- Bayer, U., Kirda, E., & Kruegel, C. (2010). **Improving the efficiency of dynamic malware analysis**. Paper presented at the Proceedings of the 2010 ACM Symposium on Applied Computing.
- Grant, T. J., Venter, H. S., & Eloff, J. H. P. (2007). **Simulating adversarial interactions between intruders and system administrators using OODA-RR**. Paper presented at the Proceedings of the 2007 annual research conference of the South African institute of computer scientists and information technologists on IT research in developing countries.
- Jamieson, R., Land, L., Smith, S., Stephens, G., & Winchester, D. (2009). **Critical infrastructure information security: Impacts of identity and related crimes**. PACIS 2009 Proceedings Association for Information Systems.
- Anwar, A. (2014). **Cyber Security of Smart Grid Infrastructure**, in The State of the Art in Intrusion Prevention and Detection, CRC Press, pp. 449-472.
- Frank L., Greitzer R. & Hohimer, E.(2011). **Modeling Human Behavior to Anticipate Insider Attacks**. *Journal of Strategic Security*, Volume IV Issue 2 2011, pp. 25-48.
- NASCIO (2012). **Cyber Security Awareness Resource Guide**
- Rivera, T. (2011). **Offensive use of virtual small arms and mitigative counterstriking**.
- Transportation Research Board Special Report 274 (2003). **Cybersecurity of Freight Information Systems**. National Research Council of the National Academies.
- Verizon (2013). **Data breach investigations report**.
- Christopher Novak (2013). **Verizon Data Breach Investigations Report Summary and Analysis**.
- Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack; Board on Energy and Environmental Systems; Division on Engineering and Physical Sciences (2012). **Terrorism and the electric power delivery**

system. National Research Council. The National Academies Press.
- Goodman, S. E. & Lin, H. S. (Eds.) (2007). T**oward a safer and more secure cyberspace**. Committee on Improving Cybersecurity Research in the United States, National Research Council. The National Academies Press.

Assignment

- **Week 3 Forum**
  - Read Frank L., Greitzer R. & Hohimer, E.(2011). **Modeling Human Behavior to Anticipate Insider Attacks**. *Journal of Strategic Security*, Volume IV Issue 2 2011, pp. 25-48.
    - What Frank, Greitzer & Hohimer (2011) argue about difficulties of picking up the trail before the fact, in order to provide time to intervene and prevent an insider cyber attack?
    - Do you agree with them? Why? Why not?
    - Respond to at least two fellow classmates' posts.

Week 4:

Topic

Emergency and Disaster Management and Cybersecurity

Technology-driven emergency management; Deterrence and emergency management; Cyber-aware emergency management; Role of knowledge acquisition and management in Emergency Management; Mitigation, Preparedness, Response, Recovery and Cyber Situational Awareness; Emergency Management and cybersecurity education; Emergency Management, Intrusions and Intrusion Detection; Boyd's OODA Loop and Emergency Management; Intra- and Interoperability; Emergency Deployment of Communications Capacity; Security of Rapidly Deployed Ad Hoc Networks; Information-Management and Decision-Support Tools; Communications with the Public During an Emergency; Emergency Sensor Deployment; Precise Location Identification, Physical Aspects of the Telecommunications Infrastructure; Regional Networks for Emergency Responders.

Learning Objectives

LO-1: Analyze cross-impact and interdependence of Cybersecurity and Emergency Management.

LO-2: Evaluate the role of information technology in Emergency Management.

LO-3: Evaluate cyber situational awareness from a mitigation, preparedness, response, and recovery standpoint.

LO-4: Assess Emergency Management Cybersecurity education.

Readings

- ***Required:*** Xia, W., Becerra-Fernandez, I., Gudi, A., & Rocha-Mier, J. (2011). **Emergency Management Task Complexity and Knowledge-Sharing Strategies**. Cutter IT Journal, 24(1), pp. 20-25.
- ***Required***: Hennessy, Patterson & Lin (Eds.) (2003), **Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, Section 2 (Types of threats associated with information technology infrastructure), Section 3.2 Systems for Emergency Response and Section 4**. National Academies Press. *(it may take a fewminutes to download and open)*.
- ***Required:*** Zibuschka, J., Laufs, U. & Roßnagel, H. (2011). **Towards ubiquitous emergency management systems**. Modiquitous 2011 Proceedings.
- ***Required:*** Amin, S., & Goldstein, M. P. (2008). **Data against natural disasters: establishing effective systems for relief, recovery, and reconstruction**. Washington DC: World Bank.
- ***Required:*** Becerra-Fernandez, I., Xia, W., Gudi, A. & Rocha, J. (2008). **Task Characteristics,**

Knowledge Sharing and Integration, and Emergency Management Performance: Research Agenda and Challenges. Proceedings of the 5th International ISCRAM Conference – Washington, DC, USA, May 2008.

Assignment

Weeks 3-4 Written Assignment (submit under Assignments)

Submit as ***single*** *MS Word document*.

Title *each* ***Part*** *below. The* ***minimum*** *approximate length for* ***both*** *Parts should be 1500 words*

- **Part 1 of 2 (refer to Week 3 Readings)**
  - Evaluate arguments and theses by

1. Clemente (2013)
2. Bellovin, Bradner, Diffie, Landau & Rexford (2011)
3. Saadawi & Jordan (2011) and
4. FEMA (2013).

Specifically, respond to the following questions:

1. **What do they in common?**
2. **What are the differences is their assessment of cybersecurity and critical infrastructure protection?**
3. **How does FEMA's Critical Infrastructure Protection Plan address key requirements set for by Clemente (2011)?**

- **Conclude with a research *or* policy question for further research**.
- You must utilize literature and cite and reference your work using **APA** style.

- **Part 2 of 2 (refer to Week 4 Readings)**

- **Evaluate**

1. **Findings and Lessons Learned in Xia, Becerra-Fernandez, Gudi, & Rocha-Mier (2011)**
2. **Information Fusion in Hennessy, Patterson & Lin (Eds.) (2003).**
3. **Can these findings be utilized in your city, county, state EOC. Why? Why not?**
4. Conclude with a research or policy question for further research

- You must utilize literature and cite properly.
  - Use **APA** style. Submit as Microsoft Word document.
  - Name the single file "*EDMG600Weeks3-4_YourLastName.doc*x" (e.g., *EDMG600Weeks3-4_Pesic.doc*x).

Week 4 Forum

Zibuschka, J., Laufs, U. & Roßnagel, H. (2011). **Towards ubiquitous emergency management systems** presented a ubiquitous emergency management system design, based on the integration of mobile and multi-touch components in the front end with sensor fusion and data mining capabilities in the back end.

- **How ubiquitous and resilient this model is?**
- **Respond to at least two fellow classmates' posts.**

Week 5:

Topic

State and Local Cybersecurity and Emergency Management Issues.

Assessment of Cybersecurity risks for state governments; Cybersecurity Management in the States, Role of Information Security Officers; Virtual Emergency Operations Center for Disaster Management Research, Training, and Discovery; Knowledge Sharing and Integration, and Emergency Management Performance; Tools for local civilian and military disaster preparedness; Meta-leadership, national emergency preparedness and government connectivity.

Learning Objectives

LO-1: Assess state and local cybersecurity challenges.

LO-2: Evaluate various models to address effective state and local cyber security challenges.

LO-3: Asses the role or Meta-leadership in government connectivity.

Readings

- **Required**: Deloitte-NASCIO (2013). **Cybersecurity Study State Governments at Risk: A Call for Collaboration and Compliance**.
- **Required:** Moore at al. (2010). **Bridging the gap: developing a tool to support local civilian and military disaster preparedness**. Santa Monica, CA: RAND (Chapters 4 & 5)
- **Required:** Marcus, L. J., Dorn, B. C. & Henderson, J.M. (2005). **Meta-leadership and national emergency preparedness strategies to build government connectivity**. Working Paper, Center for Public Leadership, Harvard University.
- **Required:** Becerra-Fernandez, I., Madey, G., Prietula, M., Rodriguez, D., Valerdi, R., & Wright, T. (2008). **Design and Development of a Virtual Emergency Operations Center for Disaster Management Research, Training, and Discovery**. Paper presented at the Proceedings of the Proceedings of the 41st Annual Hawaii International Conference on System Sciences.
- **Required**:Becerra-Fernandez, I., Xia, W., Gudi, A., & Rocha, J. (2007). **Task Characteristics, Knowledge Sharing and Integration, and Emergency Management Performance: Research Agenda and Emergency Management Challenges**. Paper presented at the 16th International Conference on Management of Technology.
- **Recommended:** Goodyear, M., Portillo, S., Goerdel, H. T., Williams, L. (2010). **Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers**. IBM Center for the Business of Government.
- **Recommended**: Bhavanishankar, R., Subramanian, C., Kumar, M., & Dugar, D. (2009). **A context aware approach to emergency management systems**. Paper presented at the Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly.

Assignment

Week 5 Forum (post under Forums)

- Discuss Meta-leadership and national emergency preparedness strategies to build government connectivity by Leonard J. Marcus, Barry C. Dorn, and Joseph M. Henderson.
  - Do you agree with authors' grounds, reasoning, claims and recommendations? Why? If not, why not?
- Respond to at least two fellow classmates' posts.

Week 6:

Topic

Industry-government partnership for cybersecurity of US Critical Infrastructure

Economics of cybersecurity: Principles and policy options; The public/private dilemma about responsibility over cybersecurity; Connecting industry to the research agenda; Organization of government in cybersecurity assurance; Organizational deficit; Cyber resilience to protect critical infrastructure; Cyber systems assurance; Identity management and authentication procedures; privacy including anonymity on the digital infrastructure; Trusted, resilient, and survivable architecture.

Learning Objectives

LO-1: Assess industry-government partnership in Cybersecurity.

LO-2: Evaluate existing and forecasting prospective solutions regarding identity management, authentication, and software and hardware resilience.

LO-3: Analyze existing solutions and recommendations for the optimal relationship between industry and government regarding Cybersecurity.

Readings

- ***Required:*** Clinton, L (2011). **Industry- Government Partnership for Cyber Defense**, *Journal of Strategic Security*, Volume 4, Number 2 , Summer 2011 (*it may take 5-6 minutes to download*
- ***Required:*** National Research Council Group (2010). Read sections "**Attribution and Economics**," (pp. 3-54) and "**The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence**," (pp. 245-272) in **Informing Strategies and Developing Options for U.S. Policy Committee on Deterring Cyberattacks**. Proceedings of a Workshop on Deterring Cyber Attacks (takes a couple of minutes to download).
- ***Required:*** **Responses to Questions** Posed by Ms. Melissa Hathaway During Her Presentation at the National Science Foundation on March 18, 2009 March 31, 2009.

Assignment

Weeks *5-6* Written Assignment

- (submit as ***single*** *MS Word file* under Assignments)
    - **Part 1 (Refer to Week *5* Readings)**
        - **After reading** Moore at al. (2010), Goodyear, Portillo, Goerdel & Williams (2010) and Deloitte-NASCIO (2013), develop a cybersecurity/EM Policy Analytical model in which you will recommend and justify the most effective way to manage emergency management related cybersecurity issues at the *state* level.
        - Utilize additional resources as needed.
        - Conclude with a *research or policy question* for further research.
        - You must utilize literature and cite properly.
        - Use **APA** style.
        - Provide *in-text citations and references*.

- **Part 2 (Refer to Week 6 Readings)**
    - **After reading the article, respond to the following *four* questions bellow.**
    - **Separate each response with the sub-headed question statement)**:
        - Larry Clinton describes government-industry partnership as similar to a parent-child relationship, wherein the parent (government) feels the need to exhibit some tough love on an uncooperative and immature child (the private sector). The analogy breaks down, however, when one realizes that in this case the "child" (industry) is actually far bigger, stronger, and has more resources than the supposed parent. Clinton argues it is the parent (government) in this case that is ultimately reliant on the child for cyber security. While industry cyber systems are vulnerable to attack-as are virtually all infrastructures historically-the market has produced an array of effective means to protect their cyber systems. The problem is the lack of proper implementation of cyber security best practices and relatively

simple fixes, like software updates and security patches. Title each response with the question text:
    - **What needs to be done and how do we get people to do it?**
    - **Will a traditional regulatory model work in this space?**
    - **Does a newer model to address uniquely 21st century issues need to be developed?**
    - **Whom should the government regulate?**
    - *Conclude* with a research or policy question for f*urther research*.
    - You must utilize literature and cite properly.
    - Use **APA** style
    - Provide *in-text citations and references*.

Submit ***both Parts as a single*** Microsoft Word document

Name the file "**EDMG600Weeks5-6_YourLastName.doc/x**" (e.g., EDMG600Weeks5-6_Pesic.doc/x). Upload the document under Assignments.

- **Week 6 Forum**
    - Read **Responses to Questions** Posed by Ms. Melissa Hathaway During Her Presentation at the National Science Foundation on March 18, 2009 March 31, 2009.
        - *Choose a question from the list, and discuss it*.
            - **Do you agree with the response? Why? Why not?**
            - **What are the gaps or weaknesses in the response?**
        - **APA**-cite and reference your response.
    - Respond to at least two fellow classmates'' posts.

Week 7:

Topic

Global cybersecurity issues and cybersecurity interdependence

Learning Objectives

LO-1:

Readings

- **Required:** Smedts, B. (2010). **Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future.** Brussels: Royal High Institute for Defence, Center for Security and Defence Studies.
- **Required:** Lieberthal, K. & Singerm, P. W. (2012). **Cybersecurity and U.S.-China Relations.** Washington, DC: Brookings.

- **Required:** Smedts, B. (2010). **Critical Infrastructure Protection Policy in the EU: State of the Art and Evolution in the (Near) Future**. Brussels: Royal High Institute for Defence, Center for Security and Defence Studies.
- **Required:** Lieberthal, K. & Singerm, P. W. (2012). **Cybersecurity and U.S.-China Relations**. Washington, DC: Brookings.
- **Required:** Forsyth, J. W. (2013). **What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace**. *Strategic Studies Quarterly,* 7, no. 1, pp. 93-113.
- **Required:** Davidson, M. A. (2009). **Monroe Doctrine in Cyberspace. Remarks made by Mary Ann Davidson in testimony given on March 10, 2009 to the Homeland Security Subcommittee on Emerging Threats, Cybersecurity and Science and Technology.**
- **Required:** Hjortdal, M. (2011). **China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence** *Journal of Strategic Security*, Volume 4 Number 2.
- Demchak, C. C., & Dombrowski, P. (2011). **Rise of a Cybered Westphalian Age**. *Strategic Studies*

Quarterly 5, no.1, pp. 32-61.
- Hurwitz, R. (2012). **Depleted Trust in the Cyber Commons**. *Strategic Studies Quarterly,* 6, no. 3, pp. 20-45.
- Knake, R. K. (2010). **Internet Governance in an Age of Cyber Insecurity**. New York: Council on Foreign Relations (may take a couple of minutes to download)
- United Nations Institute for Disarmament Research (2013). **The Cyber Index International Security Trends and Realities**.
- Center for Strategic & International Studies (2013). **Significant Cyber Incidents since 2006**.
- Tsang, F., et al. (2011). **The Impact of Information and Communication Technologies in the Middle East and North Africa**. Santa Monica: RAND.
- U.S. Director of National Intelligence (2011). National Counterintelligence Executive. **Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011**. Washington, DC: U.S. Director of National Intelligence, National Counterintelligence Executive.
- Protecting Key Assets: **A Corporate Counterintelligence Guide** (2011). Office of the Director of National Intelligence.National Counterintelligence and Security Center
- Herzog, S. (2011). **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**. *Journal of Strategic Security*, Volume 4, Number 2, Summer 2011.
- Falliere, F., Murchu, L. O, & Chien, E. (2011). **W32.Stuxnet Dossier**, Version 1.4. February 2011 (takes a couple of minutes to download).
- Glenny, M (2011). **War on the net.** Financial Times, January 28, 2011.

Assignment

Week 7 Forum

- Topic 1 of 2
  - After reading Smedts (2010), Lieberthal & Singerm (2012), and Forsyth (2013), provide a summary of issues and challenges in global cybersecurity governance.
    - Since cyberspace poses problems for international cooperation, do the problems it poses differ substantially from those governments have faced in the past?
    - Develop optimistic and pessimistic scenarios regarding global cyberspace cooperation.
    - Respond to at least two fellow classmates' posts.
- Topic 2 of 2
  - Discuss similarities and differences between U.S and EU approach to securing critical infrastructure.
  - Discuss Davidson's (2009) Cyber Monroe Doctrine.
  - After reading Hjortdal, M. (2011). *China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence,* Journal of Strategic Security, Volume 4 Number 2., how would you assess Chinese intentions and capabilities?
- Conclude with a research or policy question for further research
- You must utilize literature and cite properly. Use APA style.
- Respond to at least two fellow classmates' posts.

Week 8:

Topic

Course Wrap-up

Final Project submission

Learning Objectives

Course Reflections

Readings

No reading required.

You are encouraged to read unread supplemental resources from Weeks 1-7.

Assignment

Week 8 Written Assignment

- **Written Assignment (Final Project)** submit here
  - **IMPORTANT!**
    - Final Project must be at least 15 APA-formatted and referenced pages including title page and references.
    - You must submit your Final Project as any other Written Assignment in the course to Turn It ***through Week 8 Assignments.***
    - You can use the **template** I have developed *or* **(Research Methods) Template**
    - Final Project without a satisfactory Turn It In Similarity Index (*in the blue or green, or around **23** percent of lower*) will *not* be accepted for grading.
      - You can submit your Final Project to Turn It In through Week 8 Assignments *multiple times*. I will count your latest Final Project Turn It submission as your final submission.
    - **DO NOT SUBMIT YOUR FINAL PROJECT TO YOUR PERSONAL TURN IT IN Account or through someone else's account *before* you submit it under Week 8 Assignments.**
      - Submitting YOUR FINAL PROJECT TO YOUR PERSONAL TURN IT IN ACCOUNT or using someone else's Turn It In account will render your actual Week 8 submission ineligible for grading. It will generate 100 percent similarity (plagiarism) once (re)submitted under Week 8 Assignments.
      - Submit as Microsoft Word document.
      - Name the file "**EDMG600FinalProject_YourLastName.doc**/x" (i.e., EDMG600FinalProject _Pesic.doc/x).
      - You must use **APA** style.

- **Week 8 Forum**
  - Issues related to Cybersecurity, Critical Infrastructure protection and Emergency Management, are complex and multidimensional. They include a multitude cross-context considerations that we have only been able to start exploring, investigating and assessing. As you have realized, there is a lot more to it. I hope the Readings, Assignments, and Forums have inspired you to explore it further. Please reflect on
    - **Your most difficult part of the course.**
    - **Something you would change about the course.**
  - Respond to at least two of your classmates' posts.

Evaluation

Through weekly essay Assignment submissions, weekly Forum posts and discussion, Final Project Proposal Forum, and the course Final Project submission students will be evaluated by using the following criteria:

- **Foundation of Knowledge**
  - Beginning (1)
    - Student tries to explain some concepts, but overlooks critical details. Assignment appears vague or incomplete in various segments. Student presents concepts in isolation, and does not perceive to have a logical sequencing of ideas.
  - Developing (2)
    - The assignment reveals that the student has a general, fundamental understanding of the

course material. Whereas, there are areas of some concerning in the linkages provided between facts and supporting statements. Student generally explains concepts, but only meets the minimum requirements in this area.
    - Accomplished (3)
        - Student exhibits above average usage of subject matter in assignment. Student provides above average ability in relating course content in examples given. Details and facts presented provide an adequate presentation of student's current level of subject matter knowledge.
    - Exemplary
        - Student demonstrates proficient command of the subject matter in the assignment. Assignment shows an impressive level of depth of student's ability to relate course content to practical examples and applications. Student provides comprehensive analysis of details, facts, and concepts in a logical sequence.

- **Synthesis of Knowledge (Focus/Thesis)**
    - Beginning (1)
        - Student exhibits a limited understanding of the assignment. Reader is unable to follow the logic used for the thesis and development of key themes. Introduction of thesis is not clearly evident, and reader must look deeper to discover the focus of the writer. Student's writing is weak in the inclusion of supporting facts or statements.
    - Developing (2)
        - Student exhibits a basic understanding of the intended assignment, but the thesis is not fully supported throughout the assignment. While thesis helps to guide the development of the assignment, the reader may have some difficulty in seeing linkages between thoughts. While student has included a few supporting facts and statements, this has limited the quality of the assignment.
    - Accomplished (3)
        - Establishes a good comprehension of topic and in the building of the thesis. Student demonstrates an effective presentation of thesis, with most support statements helping to support the key focus of assignment.
    - Exemplary (4)
        - Student provides sophisticated synthesis of complex body of information in the preparation of assignment. Research provided by student contributes significantly to the development of the overall thesis. Student incorporates at least of 7-10 quality references in the development of the overall thesis. Student incorporates a variety of research resources and methodology in the preparation of assignment.
- **Application of Knowledge-Critical Thinking Skills**
    - Beginning (1)
        - Student demonstrates beginning understanding of key concepts, but overlooks critical details. Student is unable to apply information in a problem-solving fashion. Student presents confusing statements and facts in assignment. No evidence or little semblance of critical thinking skills.
    - Developing (2)
        - Student takes a common, conventional approach in guiding the reader through various linkages and connections presented in assignment. However, student presents a limited perspective on key concepts throughout assignment. Student appears to have problems applying information in a problem-solving manner.
    - Accomplished (3)
        - Student exhibits a good command of critical thinking skills in the presentation of material and supporting statements. Assignment demonstrates the student's above average use of relating concepts by using a variety of factors. Overall, student provides adequate conclusions, with 2 or fewer errors.
    - Exemplary (4)
        - Student demonstrates a higher-level of critical thinking necessary for graduate level work. Student provides a strategic approach in presenting examples of problem solving or critical thinking, while drawing logical conclusions which are not immediately obvious. Student provides well-supported ideas and reflection with a variety of current and/or world views in

the assignment. Student presents a genuine intellectual development of ideas throughout assignment.

- **Organization of Ideas/Format**
  - Beginning (1)
    - Assignment reveals formatting errors and a lack of organization. Student presents an incomplete attempt to provide linkages or explanation of key terms.
  - Developing (2)
    - Student applies some points and concepts incorrectly. Student uses a variety of formatting styles, with some inconsistencies throughout the paper. Assignment does not have a continuous pattern of logical sequencing.
  - Accomplished (3)
    - Student explains the majority of points and concepts in the assignment. Learner demonstrates a good skill level in formatting and organizing material in assignment. Student presents an above average level of preparedness, with few formatting errors.
  - Exemplary (4)
    - Student thoroughly understands and excels in explaining all major points. An original, unique, and/or imaginative approach to overall ideas, concepts, and findings is presented. Overall format of assignment includes an appropriate introduction (or abstract), well-developed paragraphs, and conclusion. Finished assignment demonstrates student's ability to plan and organize research in a logical sequence.
- **Writing Skill**
  - Beginning (1)
    - Topics, concepts, and ideas are not coherently discussed or expressed in assignments. Student's writing style is weak and needs improvement, along with numerous proofreading errors. Assignment lacks clarity, consistency, and correctness. Student needs to review and revise assignment.
  - Developing (2)
    - Assignment reflects basic writing and grammar, but with more than 5 errors. Key terms and concepts are somewhat vague and not completely explained by student. Student uses a basic vocabulary in assignment. Student's writing ability is average, but demonstrates a basic understanding of the subject matter.
  - Accomplished (3)
    - Student provides an effective display of good writing and grammar. Assignment reflects student's ability to select appropriate word usage and presents an above-average presentation of a given topic or issue. Assignment appears to be well written with no more than 3-5 errors. Student provides a good final product that covers the above-minimal requirements.
  - Exemplary (4)
    - Student demonstrates an excellent command of grammar, as well as presents research in a clear and concise writing style. Presents a thorough, extensive understanding of word usage. Student excels in the selection and development of a well- planned research assignment. Assignment is error-free and reflects student's ability to prepare graduate-level writing for possible publication in a peer-reviewed (refereed) journal.
- **Use of Technology/Applications**
  - Beginning (1)
    - Student needs to develop better formatting skills. The student may need to take additional training or obtain help from the Educator Help Desk while preparing an assignment. Research and resources presented in the assignment are limited. Student needs to expand research scope. The number of formatting errors is not acceptable.
  - Developing (2)
    - Student demonstrates a basic knowledge of computer applications. Appearance of final assignment demonstrates the student's limited ability to format and present data. Resources used in assignment are limited. Student may need to obtain further help in the use of computer applications and Internet research.
  - Accomplished (3)
    - Assignment presents an above-average use of formatting skills, with less than 3 errors. Students has a good command of computer applications to format information and/or

figures in an appropriate format. Student uses at least two types of computer applications to produce a quality assignment.
    - Exemplary (4)
        - Student provides a high-caliber, formatted assignment. Learner exhibits excellent use of computer technology in the development of assignment. Quality and appropriateness of stated references demonstrate the student's ability to use technology to conduct applicable research. Given assignment includes appropriate word processing, spreadsheet and/or other computer applications as part of the final product.
- **Research Skills**
    - Beginning (1)
        - Student fails to provide an adequate synthesis of research collected for assignment. The lack of appropriate references or source materials demonstrates the student's need for additional help or training in this area. Student needs to review and revise the assignment. The paper is not of acceptable quality for graduate-level work.
    - Developing (2)
        - Assignment provides a basic, but borderline perspective of student's research abilities. Student has incorporated less than 4 sources, which does not attempt to cover key elements of assignment.
    - Accomplished (3)
        - Student achieves an above average synthesis of research, but interpretation is narrow in scope and description within assignment. Assignment contains less than 7 resources, and presents an average overview of key concepts
    - Exemplary (4)
        - Student provides sophisticated synthesis of complex body of information in the preparation of assignment. Research provided by student contributes significantly to the development of the overall thesis. Student incorporates at least of 7-10 quality references in the development of the overall thesis. Student incorporates a variety of research resources and methodology in the preparation of assignment.

Grading:

Name	Grade %

Materials

Book Title: There are no required books for this course.

Author: No Author Specified

Publication Info:

ISBN: N/A

All course resources are open sources/public domain resources available online through individual URL links. Accessing some resources requires either signing on to APUS Library with your credentials or a free one-time web site registration. Please see each Week's Announcements and Assignments in the classroom, for each week's required and supplemental reading. Also please see Course Outline bellow.

Course Guidelines

This course requires a time management plan and the self-discipline to follow it. You are responsible for

managing your time, completing assignments on time, completing the readings, and making inquiries as needed to complete the course effectively. This is an 8-week course, which means the material must be learned in a short period of time. This requires dedication and diligence on the part of each student.

Students will follow the American Psychological Association Style Guide (APA 6th Edition) as the sole citation and reference style used in written work submitted as part of this course. Specifically, the parenthetical citations-reference list style method, which includes in-text citations with an adjoining reference list, will be utilized. Additional information concerning this writing style can be found within the APUS Library.

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals, I understand you must manage competing demands on your time. If you find that you need additional time to complete an assignment, please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade.

University Policies

Student Handbook

- Drop/Withdrawal policy
- Extension Requests
- Academic Probation
- Appeals
- Disability Accommodations

The mission of American Public University System is to provide high quality higher education with emphasis on educating the nation's military and public service communities by offering respected, relevant, accessible, affordable, and student-focused online programs that prepare students for service and leadership in a diverse, global society.