

*Syllabus for  
Technology, Terrorism and National Security Law  
[Course No. 496-001]*

**George Mason University  
School of Law  
Spring 2009**

**Professor John O. Marsh  
Professor Angeline G. Chen**

**Course Time/Location:**      Tuesdays 6:00 – 7:50 p.m.  
Room 412

**Credits/Grade:**                2 Credits

Grades will be based on class participation, a written research paper on a topic selected by each student and approved, and an in-class oral presentation. *See* section below regarding topic selection and paper requirements.

## **COURSE DESCRIPTION**

Our nation's increasing utilization, reliance and sheer dependence upon technology upon our societal infrastructure is undeniable. The pervasiveness of technological advancements has significant implications for how individuals engage in their daily lives, functioning of our economy, conduct of business by the government as well as the private sector, and – ultimately - the protection of our national interests and provision of our common defense.

One core theme of the ongoing dialogue involves recognizing that the rapid advancement of technology has led to an inextricable linking of the various systems and establishments that form the critical infrastructure and societal/philosophical underpinnings of our nation. The implications– both actual and potential – of such reliance and dependencies are far-reaching and significant.

America's critical infrastructure is comprised of those systems and assets – both physical and cyber in nature – that are so vital to our nation that their incapacitation or destruction would have an immediate and debilitating impact on our national security, national economic security and/or national public health and safety. Such systems include area sectors such as transportation, power and energy, communications, finance and banking, and emergency systems. The establishment and linking of these systems creates opportunities for business, trade, convenience, efficiency and the ability to better our lives. Exploitation of these opportunities and emergent technologies has led to America's continuing economic global dominance.

Our society's increasing dependence on technology, however, likewise opens it to vulnerability to hostile threats. Post-September 11<sup>th</sup> and in the context of the ongoing War on Terror, there can be no question that there are those that seek to attack or threaten our country through the use of any and all available means and methods. Deliberate attacks upon our national infrastructure could crash key computer-dependent control networks, such as electrical power grids, telecommunications systems and networks, transportation systems and financial institutions. A deliberate and concerted attack by a party hostile to the U.S. on one or more of these key systems, whether governmental or privately-owned, could have devastating effects. The enhancement of terrorist tools and the increase in opportunities that corresponds with the advancement of technology, its availability and its affordability likewise magnifies the potential consequences of a single event or series of attacks. The need to identify and adequately address America's vulnerabilities is thus more critical today than ever before.

In recognition of the very real threat of this facilitation of terrorism and its potential consequences through the use of advanced (and often inexpensive and readily available)

technology, the U.S. Government has issued a number of directives and regulations. Many of these directives and regulations focus on unifying governmental and private commercial sector resources in establishing a comprehensive national cyberdefense to protect the critical infrastructure of our nation, thus ensuring the continuing national security of the United States. Meanwhile, Congress, as well as state legislatures, have amended and implemented significant legislation seeking to address actual, perceived and/or anticipated deficiencies in the existing bodies of law creating the legal infrastructure upon which the societal rules of engagement rely and ensure careful consideration of integrating the components of civil liberties and homeland security. Private sector organizations and entities have likewise taken action on their own, implementing policies and establishing best practices and standards and codes of conduct that address overlapping efforts relating to business continuity and disaster recovery. Finally, other nations and global actors also have taken steps to attempt to address the recognized threat of disruption and catastrophic consequences of a direct and concerted attack upon critical infrastructure assets around the world.

While many of the consequences of these efforts align with the overarching objective of understanding and protecting the physical and economic infrastructure that serves as the backbone of our country's national security, it is important to recognize that such efforts are focused on other objectives and can also create conflict and contradictions, and that there is no "one-size-fits-all" solution. Comprehensive and multi-faceted risk management is thus all the more complex, and yet all the more critical.

In such a dynamic environment, a thorough and ongoing analysis of how to ensure appropriate consideration of the most effective means of protecting American society and concurrently recognizing and preserving the individual civil liberties that underpin our way of life in this country is critical. The convergence of the real and perceived threats of terrorism, the advancement of sophisticated and readily available technologies, and America's dedication to preserving the civil liberties of its citizens alongside the obligation to ensure our country's national security gives rise to a significant number of legal issues of first impression. Moreover, as the relevant technology continues to develop rapidly, the ability of the law to keep pace or anticipate dynamic situations is often severely stretched, and the readiness of the legal profession to be a valued partner to our nation is constantly challenged.

This course will explore the existing laws, equities and variables in this compelling multidisciplinary area, along with the tensions that are created as a result of the various competing concerns, in an interactive manner. We will draw upon the expertise of outside individuals with significant experience, as well as the experiences of the students in the class. Throughout the semester, we will also weave strategic planning, risk management, economical considerations and real-world application into our discussions of the legal issues and challenges.

**Class Attendance:** Consistent with law school policy, regular and punctual attendance is required. If absence is unavoidable, prior arrangements must be made with the professors where possible. If for some reason you are unable to contact one of us prior to any absence, please do so as soon as practicable. Unexcused absences from this class may affect your grade in this course.

**Office Hours:** Professors Marsh and Chen do not have set office hours on-campus. Appointments should therefore be requested and made in advance, and are more easily managed via phone. Outside of class, Professor Chen can be reached either via e-mail: [angeline.g.chen@lmco.com](mailto:angeline.g.chen@lmco.com) or via phone: (301) 897-6229.

**Class Format:** Class format will consist of a combination of presentations by the professors and various guest lecturers, combined with class discussions regarding the presentations provided as well as the assigned or recommended reading materials for that class. Guest lecturers are distinguished individuals with established expertise directly in or relevant to the specific focus for that particular class. *Remarks are not for attribution unless otherwise expressly noted.*

**Tape Recording:** Tape recording of any class session is strictly prohibited.

**In-class Laptop Usage:** Note-taking during class using personal laptops is permissible. *Accessing and use of the GMU wireless area network during class, however, is not permitted while class is in session. Particularly when we have guest lecturers with us, please accord them due courtesy and the attention they deserve, and refrain from using your laptops for any other use than taking notes on the remarks being given.*

## LEGAL RESEARCH PAPER AND PRESENTATIONS

A legal research paper and an in-class oral presentation are required in lieu of a written examination. It is recommended that you begin considering your topic selection for the paper as soon as possible in order to avoid last-minute scrambles towards the end of the semester and to allow time for sufficient substantive research.

**Paper Requirements:** The paper should be approximately 25-35 double spaced pages, and must reflect individual substantive research on and analysis of a legal issue relevant to the subject matter of this course. You are free to select a topic of your choice, but must have the topic selected and approved by the professors in accordance with the schedule set forth herein. *Your intended topic and a rough outline of your proposed paper must be submitted for review and approval by no later than 17 February 2009.*

**Citation Format:** Papers should be well-organized, written and citations properly formatted in accordance with the current version of the Blue Book. Endnotes should be utilized, and should appear at the end of the paper.

**Executive Summary:** An executive summary or abstract of the paper's premise and analysis (of approximately 1-2 pages in length and independent of the paper itself) must also be submitted along with your finished paper. The executive summary and the endnotes are not counted towards the page count for your final paper.

**Submission:** Final papers and executive summaries should be submitted via e-mail to Professor Chen at [angeline.g.chen@lmco.com](mailto:angeline.g.chen@lmco.com) (Professor Chen will provide you either an

e-mail or telephonic confirmation of receipt of your paper). Alternative means of submission require advance notice and arrangements.

Please be sure that all of your materials are clearly marked with your name and semester. Because you will be submitting a paper, examination numbers are not required. Contact information for the student (phone number and e-mail address) should also be provided on the front page of the paper and the Executive Summary.

**PAPERS ARE DUE ON TUESDAY, 5 MAY 2009.**

**Presentation Requirements:** In-class oral presentations will take place during the last three class sessions (April 7<sup>th</sup>, 14<sup>th</sup>, and 21<sup>st</sup>). Presentations should be approximately 10-12 minutes in length, depending on the number of students in the class, and will be scheduled in advance during one of the prior classes via sign-up by students for scheduled dates and time slots. The amount of time available for each presentation may be adjusted due to the number of students in the class; the professors will inform the class of the specific time limit by no later than November 4<sup>th</sup>. Students should be sure to plan on adhering to noted time limitations. The use of PowerPoint or other visual aids to supplement presentations is permitted but not required.

## **COMPILATION OF RECOMMENDED READING MATERIALS AND SEGMENTS**

Due to the nature of this course, there is no assigned text and no set weekly reading assignments. A CD-ROM containing a compilation of recommended reading, key resources and other relevant materials will be provided to the class by the professors. *The compilation is strictly for your personal use in conjunction with this class.* This approach was taken to assist students in saving costs for reading materials.

**The compilation is presented in components sequentially ordered solely for your consideration in reviewing the materials, they do not have to be reviewed in order (unless specifically assigned).**

Specific reading assignments, if any, will be based primarily upon the materials provided either by the professors in class or as cited in the reading list. Occasionally, supplemental materials may be placed on Reserve in the GMU Library by the professors.

**Please Note:** Where cited materials are marked with an asterisk, this means that they are available via WestLaw, LEXIS or the Internet as noted and are *not* included in the CD compilation provided by the professors. Students desiring to review such materials are responsible for acquiring electronically available materials via the resources provided to them as GMU students.

## TECHNOLOGY, TERRORISM AND NATIONAL SECURITY LAW SEMINAR SPRING 2009 SUPPLEMENTAL READING MATERIALS COMPILATION

Materials contained in the compilation are divided into two groups: General Materials, which provide key background information, context and resource materials that support the entire course scope, and Component Segments, which provide more focused materials in specific areas intended to be covered or otherwise touched throughout the semester. Other than the General Materials, which should be reviewed first, you are encouraged to review the reading materials by subject matter and interest rather than in the sequence set forth below.

### GENERAL REFERENCE MATERIALS

- The U.S. Constitution (Articles I, II, III and IV and the 4<sup>th</sup> Amendment)
- PCCIP Legal Foundation Reports (1997)
- \*The 9/11 Commission Report, located at <http://www.9-11commission.gov/>
- Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence (February 2, 2006)
- National Intelligence Estimate (July 2007)
- Markle Foundaition Reports on a Trusted Network for Homeland Security (Volumes I, II and III)
- National Infrastructure Protection Plan, Department of Homeland Security (2006)
- The Intelligence Reform and Terrorism Prevention Act of 2004, PL 108-458
- Rand White Paper: Compendium of Public and Private Organizations' Policy Recommendations, Rand Organization (2003)
- Department of State, Office of the Coordinator for Counterterrorism, Country Terrorism Reports 2005 (April 2006)
- National Commission on Terrorist Attacks Monograph on Terrorist Financing (Staff Report to the Commission)
- National Strategy to Secure Cyberspace (February 2003)
- National Strategy for the Physical Protection of Critical Infrastructures and Key Assets (February 2003)
- National Strategy for Homeland Security (July 2002)
- National Response Plan (December 2004)
- USA Patriot Act (26 October 2001) and summary (.html format)
- Security in the Information Age, Congressional Joint Economic Committee Report (May 2002)

### COMPONENT SEGMENT MATERIALS

#### **COMPONENT ONE: COMPUTER AND INTERNET SECURITY**

- Federal Information Systems Management Act of 2002, 44 USC § 3541, *et seq.*
- Homeland Security Act, PL 107-296 (2002)
- E-Government Act, PL 107-347 (2002)

- Lipson, H.F. Tracking and Tracing Cyber-attacks: Technical Challenges and Global Policy Issues (November 2002)
- Hennessy, J.L., Patterson, D.A. and Lin, H.S. (eds). Information Technology for Counterterrorism: Immediate Actions and Future Possibilities. (National Research Council: National Academies Press). Available on-line at: [http://bob.nap.edu/html/IT\\_counterterror/](http://bob.nap.edu/html/IT_counterterror/)
- \*Hennessy, J.L., Patterson, D.A. and Lin, H.S. (eds). Cryptography's Role in Securing the Information Society. (National Research Council: National Academies Press). Available on-line at: <http://www.nap.edu/catalog/5131.html>.
- Computer Security Act of 1987, 15 U.S.C. § 278 and *Legislative History*
- CSIS Report: Cyber Threats and Information Security: Meeting the 21<sup>st</sup> Century Challenge (May 2001)
- White Paper on Cyberterror: Prospects and Implications, Center for the Study of Terrorism and Irregular Warfare, Monterey, CA (October 1999)
- GAO Testimony of David L. McClure Before the Subcommittee on Government Management, Information and Technology, Comm. On Gov't Reform, House of Rep., *Federal Chief Information Officer: Leadership Needed to Confront Serious Challenges and Emerging Issues* (12 Sept. 2000)
- \*Stevan R. Salbu, *Who Should Govern the Internet?: Monitoring and Supporting a New Frontier*, 11 Harv. J.L. & Tech. 429 (1998)
- Senator Kyl report on Cyber Crime (November 1998)
- United Nations Guidelines for the Regulation of Computerized Personal Data Files, *UNGA 45/95* (14 December 1990)
- Richmond, R., *Anatomy of a Threat*, Wall Street Journal Online (February 13, 2006)
- \*Overview of the IETF, located at <http://www.ietf.org/overview.html>
- \*IETF Wiretapping Policy, located at <http://www.ietf.org/rfc/rfc2804.txt>

## **COMPONENT TWO: POLICY, LEGISLATION AND OVERSIGHT: THE ROLES OF CONGRESS, USG AGENCIES AND STATE GOVERNMENTS**

- \*The U.S. Constitution – Articles I, II, III and IV and the 4<sup>th</sup> Amendment
- About the Constitution, Department of State Bureau of International Information Programs (2004)
- *Youngstown Sheet & Tube Co. v. Sawyer*, 343 US 579 (1952)
- \*Outline of U.S. Government (Chapter 4, The Legislative Branch: The Reach of Congress), located at <http://usinfo.state.gov/products/pubs/outusgov/>
- \*USG Manual, located at <http://www.gpoaccess.gov/gmanual/browse-gm-01.html>
- Department of Homeland Security Organizational Chart (August 2004)
- Office of Management and Budget 2003 Report to Congress on Combating Terrorism (September 2003)
- Homeland Security Act of 2002 (HR 5005)
- Office of Management and Budget Statement on H.R. 5005, Homeland Security Act of 2002 (25 July 2002)
- Homeland Security Presidential Directive 2 (October 2001)
- White Paper on Presidential Authority over NSA Activities, Department of Justice (January 19, 2006)

- CRS Memorandum regarding Presidential Authority to Conduct Warrantless Surveillance to Gather Foreign Intelligence Information (January 5, 2006)

### **COMPONENT THREE: RISK IDENTIFICATION, ASSESSMENT AND MANAGEMENT**

- Estimating Terrorism Risk, Rand Corporation Report and Summary (2006)
- Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructures, GAO Report (December 2005)
- Terrorism Risk Insurance Act of 2002, PL 107-297 (November 26, 2002)
- Insurance Sector Preparedness, GAO Report (November 2005)
- US and European Approaches to Insure Natural Catastrophe and Terrorism Risks, GAO Report (February 2005)
- HIPAA Security Regulations, 45 CFR Parts 160, 162 and 164 (Feb 2003)
- Gramm-Leach-Bliley Act, Report 106-434, 106 Cong. 1<sup>st</sup> Sess. (2 Nov. 1999)
- *Gramm-Leach-Bliley Security Regulations and Guidelines*, Department of the Treasury, Office of the Comptroller of the Currency (June 26, 2000)
- Office of the Comptroller Interagency Guidelines Establishing Standards for Safeguarding Customer Information Proposed Rule (26 June 2000)
- \*FTC Standards for Safeguarding Customer Information: Proposed Rule, 16 CFR Part 314, located at <http://www.ftc.gov/os/2001/07/stansafecustinfofrn.htm>
- Cong. Testimony of B. Schneier before the Science, Tech & Space Subcommittee of Sen. Comm. (Comm, Science & Transp), *E-Commerce Security Risks* (July 16, 2001)
- OECD Report on Promoting a Culture of Security for Information Systems and Networks in OECD Countries (16 December 2005)
- *Computer Owners Face Liability*, NYLJ, Vol. 224 No. 29 (Aug. 11, 2000)
- *Firms May Be Liable*, NY Law Journal, Vol. 223 No. 41 (Mar. 2, 2000)

### **COMPONENT FOUR: INFORMATION ANALYSIS, ASSURANCE AND SECURITY**

- Information Management for Net-centric Operations, Defense Science Board 2006 Summer Study Volume I, Main Report (April 2007)
- Information Sharing: Federal Government Needs to Establish Policies and Processes for Sharing Terrorism-Related and Sensitive but Unclassified Information, GAO Report (March 2006)
- National Information Assurance Strategy (UK Central Sponsor for Information Assurance 2007)
- Rogers, L.R., Principles of Survivability and Information Assurance, Carnegie Mellon: 2004
- Protection of Classified Information, CRS Report (June 30, 2006)
- National Industrial Security Program Operating Manual, DoD 5220.22-M (February 28, 2006)
- Lewis, J., CSIS Paper on CFIUS (February 2006)
- Critical Infrastructure Information Act of 2002
- Wassenaar Arrangement Basic Documents (January 2006)

- \*Department of Justice FAQ on Encryption Policy (April 24, 1998)  
<http://www.usdoj.gov/criminal/cybercrime/cryptfaq.htm>
- \* Export Admin Regs (EAR) Pt 730 (Gen'l Info) & Pt 736 (Gen'l Prohibitions), at <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=bx&docid=f:730.pdf> and <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=bx&docid=f:736.pdf>, respectively, (just skim over on-line)
- \*International Traffic in Arms Regulations, located at <http://www.pmdtc.gov> (under "Quick Links" click on 'Regulations: ITAR'; just skim over on-line)
- \*Economic Espionage Act of 1996, *Legislative History*, located at <http://www.cybercrime.gov/eea.html>
- \*The Computer Science and Telecommunications Board, National Research Council Report "Cryptography's Role In Securing the Information Society" located at <http://www.nap.edu/readingroom/books/crisis/>
- OECD Guidelines for Cryptography Policy (1997)
- Shimeall, T. *et al.*, *Combating CyberWar*, *Nato Review* (Winter 2001/2002)
- \**U.S. v. Morison*, 844 F.2d 1057 (4<sup>th</sup> Cir. 1988)
- \**New York Times Co. v. United States*, 403 U.S. 713 (1971)
- \*Allen M. Shinn, *The First Amendment and the Export Laws: Free Speech on Scientific and Technical Matters*, 58 Geo. Wash. L. Rev. 368 (1990)

## **COMPONENT FIVE: PRIVACY**

- Privacy: Lessons Learned About Data Breach Notifications (GAO Report 2007)
- Rosenzweig, P. (August 7, 2003) Proposals for implementing the TIA System. Legal Memorandum Executive Summary (The Heritage Foundation) No. 8.
- Anti-Terrorism and Effective Death Penalty Act, 8 U.S.C. 1189
- Privacy: Preventing and responding to the improper disclosures of personal information, Statement of David M. Walker, Comptroller General of the US (June 8, 2006)
- \*OECD Guidelines on the Protection of Privacy & Transborder Flows of Personal Data, located at <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>
- *The Defense of Privacy Act and Privacy in the Hands of the Government*, Testimony of James X. Dempsey, Executive Director, CDT before the Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution of the House Judiciary Committee (July 22, 2003)
- *The Carnivore Controversy: Electronic Surveillance and Privacy in the Digital Age*, Testimony of James X. Dempsey, Senior Staff Counsel, Center for Democracy and Technology before the Sen. Judiciary Comm. (Sept. 6, 2000)
- Jerry Berman and Lara Flint, [\*Guiding Lights: Intelligence Oversight and Control for the Challenge of Terrorism\*](#) *Criminal Justice Ethics*, Vol. 22, No. 1 (Winter/Spring, 2003)
- \*Michael J. O'Neil & James X. Dempsey, *Critical Infrastructure Protection: Threats to Privacy and Other Civil Liberties and Concerns with Government Mandates on Industry*, 12 DePaul Bus. L.J. 97 (1999/2000)

- *\*Internet Security and Privacy*, Testimony of James X. Dempsey, Sr. Staff Counsel, Center for Democracy and Technology before the Sen. Judiciary Comm. (May 25, 2000), located at <http://www.senate.gov/~judiciary/52520jxd.htm>

## **COMPONENT SIX: CRITICAL INFRASTRUCTURE PROTECTION: SCOPE AND STRATEGY**

- Critical Infrastructure Protection: DHS Faces Challenges in Fulfilling Cybersecurity Challenges, GAO Report (May 2005)
- Critical Infrastructure Protection: Challenges in Securing Control Systems, Statement of Robert Dacey, GAO (October 1, 2003)
- Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors, GAO Report (July 2004)
- Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities (January 2001)
- HSPD-7, Critical Infrastructure Identification, Prioritization and Protection (December 17, 2003)
- \*Presidential Decision Directive 63 (May 22 1998), located at <http://www.fas.org/irp/offdocs/pdd/pdd-63.htm>
- White Paper on PDD 63 (May 22, 1998)
- Executive Order 13231, Critical Infrastructure Protection in the Information Age (October 18, 2001)
- Report to the President's Commission on Critical Infrastructure Protection: Studies and Conclusions [Report 1 of 12] (1997)
- House Hearings on the Marsh PCCIP Commission (November 1997)
- GAO Testimony on CIP Governance Problems (July 2000)
- Interim Report: Causes of the August 14<sup>th</sup> Blackout in the United States and Canada (Nov 2003)
- Congressional Research Service Report (Critical Infrastructure Background and Implementation of PDD-63) (updated July 12, 2005)

## **COMPONENT SEVEN: LAW ENFORCEMENT, INTELLIGENCE AND NATIONAL DEFENSE**

- Joint Inquiry into the Terrorist Acts of September 11, 2001 by the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence (December 2002)
- National Security Act of 1947
- Executive Order 12333
- Lewis, J. *Why can't the US have its own MI5?* (CSIS August 2006)
- Intelligence Issues for Congress, CRS Report (April 10, 2006)
- Opening statement by Michael V. Hayden before the Senate Select Committee on Intelligence (May 18, 2006)
- Intelligence and Security Committee (UK) Report on London Attacks on July 7, 2005 (May 2006)
- *In Re: All Matters Submitted to the FISA Court* (FISA Ct. Opin., 17 May 2002)

- Foreign Intelligence Surveillance Act, 50 USC § 1801 *et seq.* (1978)
- Foreign Intelligence Surveillance Act of 1978 (FISA), *Legislative History*
- \*Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793 (1989)
- \*Lawrence D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 Duke L.J. 1467 (2001)
- Communications Assistance for Law Enforcement Act-CALEA: Flexible Deployment Assistance Guide
- \*M. E. Bowman, *The Military Role in Meeting the Threat of Domestic Terrorism*, 39 Naval L. Rev. 209 (1990)

### **COMPONENT EIGHT: INTERNATIONAL RULE OF LAW, LAWS OF ARMED CONFLICT, GLOBALIZATION AND TRADE CONTROLS**

- \*The United Nations Charter [Articles 2(4), 51, 53, 106 & 107 and Chapter VII], located at <http://www.un.org/aboutun/charter/index.html>
- Joint Publication 3.13-1, *Electronic Warfare* (25 January 2007)
- UN Report on Threats and Challenges (2004)
- [National Security Strategy of the United States of America](#), by George W. Bush, The White House (September 20, 2002)
- *Combating Terrorism: Determining and Reporting Federal Funding Data*, GAO Report (January 2006)
- Haveman, J.D. *et al.*, *U.S. Port Security Policy after 9/11: Overview and Evaluation*, 2 J. Homeland Sec. and Emer. Management 4 (2005)
- Lewis, J. CSIS Paper on COE Cybercrime Convention (January 2004)
- \*Council of Europe Convention on Cybercrime (10 July 2001) and FAQ sheet, located at <http://www.cybercrime.gov/intl.html#Va>
- *The New National Security Strategy and Pre-Emption*, draft Brookings Institution Policy Brief (2003)
- *Creating a Safer Information Society*, European Commission Report (2002)
- *Network and Information Security: Proposal for a European Policy Approach*, European Commission Report (6 June 2001)
- Statement of Mark Richard, US DOJ, presented at EU Forum on Cybercrime in Brussels, Belgium (27 November 2001)
- *Cyberwarfare*, S. Hildreth, Congressional Research Service (November 2000)
- DoD Information Operations policy perspectives: Department of Defense, *Joint Doctrine of Information Operations, Chapter II, Offensive Operations*, Joint Pub 3-13 (October 9, 1998)
- Hitt, G., *U.S. Foreign Investment Debate Goes Global*, Wall Street Journal Online (May 30, 2006)
- \*Abraham D. Sofaer *et. al*, *A Proposal for an International Convention on Cyber Crime and Terrorism*, Joint Report by the Hoover Institution, CRISP, CISAC and Stanford University (August 2000), located at <http://www.oas.org/juridico/english/monograph.htm>

- Department of Treasury, Office of Foreign Assets Control, *located at* <http://www.treas.gov/offices/enforcement/ofac/>

### **COMPONENT NINE: PUBLIC/PRIVATE COORDINATION AND COOPERATION**

- Information Sharing: Protecting and Sharing Critical Infrastructure Information, GAO Report (April 2006)
- Flynn, S.E. & Prieto, D.B., *Neglected Defense: Mobilizing the Private Sector to Support Homeland Security*, CSR No. 13, Council of For. Relations (March 2006)
- Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan, GAO Report (June 2006)
- *Untangling the Web: Congressional Oversight and DHS*, Business Executives for National Security White Paper (December 10, 2004)
- *Company Primer on Preparedness and Response Planning for Terrorist and Bioterrorist Attacks*, Business Executives for National Security (2004)
- \*Report to the President’s Commission on Critical Infrastructure Protection: Privacy Laws and the Employer-Employee Relationship [Report 9 of 12] (1997), located at <http://www.ciao.gov/PCCIP/lf09.pdf>
- \*The International Economic Emergency Powers Act, Pub. L. No. 95-223, 91 Stat. 1625 (1977), *codified at* 50 U.S.C. §§ 1701 – 1706
- \*Brian A. Persico, *Under Siege: The Jurisdictional and Interagency Problems of Protecting the National Information Infrastructure*, 7 Comm. Law. Prospectus 153 (1999)
- Terrorism Risk Insurance Act, PL 107-297 (26 November 2002)
- GAO Report on Insurance Sector Preparedness (November 2005)
- ABA International Guide to Combating Cybercrime (Version 8 draft)

### **COMPONENT TEN: STRATEGIC PLANNING AND RESPONSE MANAGEMENT**

- Homeland Security: Preparing for and responding to disasters, Statement of William O. Jenkins, Jr. (GAO Report, March 2007)Black Dawn Scenario-Based Exercise (Brussels, Belgium: May 3, 2004)
- National Response Plan (December 2004)
- Harvard Long-term Legal Strategy Project Report (Nov. 2004)
- \*National Emergencies Act, *codified at* 50 USC §§ 1601 – 1651
- \*The Robert T. Stafford Disaster Relief and Emergency Assistance Act (“The Stafford Act”), PL 93-288, *as amended*
- FEMA: Factors for Future Success and Issues to Consider for Organizational Placement, GAO Report (May 9, 2006)
- \*“Emergency Responders: Drastically Underfunded, Dangerously Unprepared” Independent Task Force, Council on Foreign Relation Report (July 2003), located at [http://www.cfr.org/content/publications/attachments/Responders\\_TF.pdf](http://www.cfr.org/content/publications/attachments/Responders_TF.pdf)
- Statement of Randall A. Yim, Managing Director on Homeland Security and Justice Issues, “Combating Terrorism, Evaluation of Selected Characteristics in National Strategies Related to Terrorism” GAO 04-408T (3 February 2004)

- Joint Congressional Inquiry Report of the U.S. House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence on the Terrorist Attacks of 9/11 (24 July 2003)
- Homeland Security Presidential Directive 3 (2002)
- Frank Hoffman, *Homeland Security: A Competitive Strategies Approach* (CDI: March 2002) – excerpts
- Organizing for Homeland Security, Rand Corporation Publications Issue Paper (2002)
- \*Barry Kellman, *Catastrophic Terrorism – Thinking Fearfully, Acting Legally*, 20 Mich. J. Int'l L. 537 (1999)
- Chris Seiple, *Consequence Management: Domestic Response to Weapons of Mass Destruction*, Parameters 88-109 (Autumn 1997)

## **REMINDERS:**

Paper topics due: February 17<sup>th</sup> [via e-mail preferred]

In-class presentations: April 7<sup>th</sup>, 14<sup>th</sup>, and 21<sup>st</sup>

**Executive Summaries and Final Papers due: 5 May 2009, Tuesday**

[Electronic submission preferred, advance notice of alternative submission means required]