This course will look at the growth and scope of cyber warfare as it impacts national power in the realms of government, diplomacy, international law, international commerce/economic power, social media/privacy, science/technology, and civil society. It traces the evolution of conflict from traditional information gathering to the development of cyber weaponry with destructive capabilities and the use of those capabilities to advance national foreign policy interests. Through the use of case studies and selective readings from a variety of sources (government policy directives, cyber security industry studies, and defense related academic papers) the course guides students through the emergent quality of the broadening scope of cyber conflict and the multifaceted response to the challenge. Ultimately students are confronted with the impact of the ongoing threat as they interface with cyberspace in their day-to-day interactions. The goal is for a deeper understanding of the scope and complexity of the cyber domain and the global conflict that is raging out of view.

E-mail: bottse@stthom.edu  
Phone: (713) 525-3530  
Office Hours: By Appointment  

Text:  

Assigned Required Readings:

- NIST Cyber Security Framework 2014,  
- Federal Information Security Management Act (2002),  
- Federal Information Security Modernization Act (2014) as Amended,
Presidential Policy Directive 2013-03915, Executive Order 13636 Improving Critical Infrastructure Cyber Security,

Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization, Center for International and Strategic Studies, James A Lewis & Katrina Timlin 2011,

McAfee – Net Losses: Estimating the Global Cost of Cybercrime, Economic Impact of Cybercrime II, Center for Strategic and International Studies, June 2014,

Information Operations Warfare And Asymmetric Warfare…Are We Ready, by LTC McWarren V. Patterson U.S. Army U.S. Army War College, April 2002, Abstract,

Cyber War jfq-79_46-53, Strategic Development of Special Warfare in Cyberspace by Patrick Michael Duggan, JFQ; 4th Quarter 2015.

National Defense University JFQ 73. 2nd Quarter 2014, Sun Tzu in Contemporary Chinese Strategy by Fumio Ota


Cyber incident readings: emerging threats/dynamic response – posted each class on Blackboard.

Recommended Readings:

OSAC (Department of State, Bureau of Diplomatic Security) Overseas Advisory Council, Country Cyber Risk Analysis, retrieved 3/25/2015,

FBI Public Service Announcement – Internet of Things, September 10, 2015 Alert Number 1-091015-PSA,

Detangling the Web A Screenshot of U.S. Government Cyber Activity, National Defense University. jfq-78_78-83, G. Alexander Crowther & Shaheen Ghori, 2015,

Department of Homeland Security National Infrastructure Protection Program (NIPP), Supplemental Tool: Connecting to the NICC and NCCIC, 2013,


GRADUATE STUDENTS

NOTE: GRADUATE STUDENTS NEED TO CONSULT WITH THE INSTRUCTOR FOR ADDITIONAL REQUIREMENTS. The quality of work from graduate students should be, by definition, superior to undergraduate work. Graduate students:

• Will be required to make a presentation and lead a class discussion on a topic determined by the instructor and are encouraged to meet with me to discuss course material at greater length and outline presentation preparation.
• should exhibit a greater ability to summarize and synthesize information.
• are expected to read all articles posted on Blackboard.
• are expected to contribute to class discussion on a regular basis.
On examinations, graduate students will also be held to a higher standard with regard to the precision of answers, quality of written submissions in terms of writing clarity, organization of argumentative supposition, and the efficacy of cited sources. Partial credit will be limited.

Graduate Required Readings:


Web Site: Blackboard through the University of St. Thomas web site

Attendance: Attendance is required

Assessment/Grades:  

Mid-term Examination – 20%

In class Quizzes (2 x 5%) – 10%

Essays: Case studies (2 x 10%) – 20% (select a cyber war case study from a public source, write a 3 page synopsis/summary and identify the impact on U.S. national security interests)

Class participation – 10% (attendance & discussions of current events articles from various sources)

Final Exam paper: 40% - Select a THREAT: Foreign Hostile intelligence, Cyber-criminal organization(s), or Hacktivists and identify the potential target of the threat, explain the VULNERABILITY of the target to attack, outline the RISK of the attack to the national security/critical infrastructure of the U.S. and what steps that can and should be taken to prepare for and mitigate the impact of the attack. Draft your conclusions in a 5-7 page report using APA style, double spaced, 12 font Times New Roman format. Cite at least three sources. Include a title/cover page and reference page.
**Students With Disabilities**

Any student with a documented disability needing academic accommodations is requested to speak with me as early as possible. All discussions will remain confidential. Students with disabilities will also need to contact Counseling and Disability Services in Crooker Center. This office can be reached at (713) 525-3162 or 6953. Additionally, you will need to register with the Counseling and Disability Services Office in Crooker Center; a professor is unable to unilaterally grant ADA consideration to students.

******

**Plagiarism**

Plagiarism is a representation of another person's work as your own (for example, directly quoting from another source without using quotation marks). See the University of St. Thomas' Regulation on “Scholastic Dishonesty” for discussion and range of available penalties. Plagiarism will be punished to the maximum extent possible. If a student is found to have committed an act of scholastic dishonesty, I will recommend the most severe penalty.

**NOTE: International Studies Departmental Policy: Late Work**

The acceptance of late projects and subsequent penalties is subject to the International Studies Department policy. If unable to submit assigned work on time due to medical or serious family circumstances, prior to the due date of the paper the student must contact the professor promptly via email, office visit or telephone and provide a description of the circumstances (faculty confirmation receipt reply required). The professor’s decision based on merits of the request will be communicated to students via email.

If an extension has not been granted by the professor, late work is subject to the following penalties:

1) One letter grade (10 pts.) within the first 24-hour period, **which starts at the beginning of the class on the date due**. This means 3:10 p.m. sharp.

2) An additional letter grade for the period after 24 hours late and prior to the end of the seventh day late.

3) After a total of seven days late (including weekends), the required assignment will not be accepted and a "0" will be assigned for that assignment.
Learning Outcomes: 1. Provide a broader understanding of the global information infrastructure (cyberspace) and the dependence established public/private nation-state institutions have on that infrastructure for national power.

2. Assist students in understanding the role information warfare plays in the competition between states and non-state institutions as they seek to enhance power and influence to shape the course of world events.

3. Establish a conceptual framework that demonstrates the scope and complexity of information technology as an aspect of state power and the threats, vulnerabilities, and risks to established public/private institutions from individuals and entities, both state and non-state actors.

4. Demonstrate that cyberspace has become a warfighting domain and that active conflict is occurring within that domain which has and will have an impact on national power.

Course Conceptual Outline

Section I – Defining the Battlespace: Why cyberspace has emerged as a conflict zone (Class 1 – 5)

Section II – The Cast of Characters: State and Non-State Actors (Class 6 – 14)

Section III – Responding to the Challenge: A multi-dimensional conflict (Class 16 – 21)

Section IV – The New Cyber World Order: War on the Homefront (Class 22 – 29)

Class Schedule:

Class 1 – August 22: Brief overview of the historical foundations of the evolution of warfare through the concept of the 5 dimensional battlespace. Administrative Day – Class introductions, instructor/student expectations and introductory lecture notes


Class 12 – October 3: Chinese Cyber War Doctrine – Sun Tzu and the Art of Cyber War. Readings: (post of blackboard) National Defense University JFQ 73. 2nd Quarter 2014, Sun Tzu in Contemporary Chinese Strategy by Fumio Ota

Class 13 – October 5: North Korea – Sony Hack (Quiz) Readings: TBA – Graduate Lecture Presentation


Class 15 – October 17: Mid-Term Examination


Class 18 – October 29: Business Fights Back: NERC, ISO 27000 – Compliance and security best practices. (case study assignment # 2 - select a cyber war/cybercrime case study from a public source, write a 3 page synopsis/summary and identify the impact on national security interests: APA - double spaced 12 font Times New Roman– cite source and include title page). In class presentation & lecture notes -presentation posted on blackboard.


Class 22 – November 9: Privacy, Censorship, and Net Neutrality (discuss final paper re: progress - 2nd case study assignment due) In-class roundtable discussion. Discussion topics: TBA (Apple v. FBI)

Class 23 – November 14: The Dark Web In class presentation & lecture notes - presentation posted on blackboard.

Class 24 – November 16: Dissecting the Internet of Things – IoT In-class presentation & lecture notes -presentation posted on blackboard.


