Syllabus

Listen

Syllabus

POL-380: Foundations of Cybersecurity Policy

Written By:
Joed Carbonell-López, Ph.D.
Chadd Carr, Ph.D.

Course Description

Students in this course will identify and evaluate U.S. and international cybersecurity policy within an international relations context. Students will identify key traits of effective cybersecurity policy and analyze its integration into international relations strategy. Students will develop cybersecurity policy for any given nation or international organization and analyze its impact on its foreign relations. This course will integrate legal, ethical, and biblical frameworks with the analysis of cybersecurity policy.

Credit Hours: 3
Prerequisite Courses: None

Course Outcomes

Upon successful completion of this course, you should be able to:

1. Analyze the role of cybersecurity policy in the U.S. national security strategy formation process.
2. Identify the components of an effective, international cybersecurity policy.
3. Integrate legal, ethical, and biblical frameworks with the analysis of cybersecurity policy.
4. Demonstrate the ability to research and analyze U.S., regional, and international cybersecurity policy.
5. Evaluate cybersecurity policies of international and non-governmental organizations.
6. Analyze the role and impact cybersecurity policy can have on a nation's foreign policy.

Course Textbooks

Easttom, C. (2016). Computer security fundamentals. Indianapolis, IN: Pearson.

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). Cybercrime and digital forensics. New York, NY: Routledge.

Libicki, M. C. (2016). Cyberspace in peace and war. Annapolis, MD: Naval Institute Press.

Grading Scale

NOTE: In graduate level courses, a grade of C- or below will require the course to be repeated.

Grade	Quality Points Per Credit	Percentage	Score
A	4.0	95%–100%	950–1000
A-	3.7	92%–94.9%	920–949
B+	3.3	89%–91.9%	890–919
B	3.0	85%–88.9%	850–889
B-	2.7	82%–84.9%	820–849
C+	2.3	79%–81.9%	790–819
C	2.0	75%–78.9%	750–789
C-	1.7	72%–74.9%	720–749
D+	1.3	69%–71.9%	690–719
D	1.0	65%–68.9%	650–689
F	0.0	0%–64.9%	0–649

Grading Policies

Your grading policy for your course is dependent on your school and program. Your grading policies can be found in the IWU Catalog.

Letter Grade Equivalencies

NOTE: In graduate level courses, a grade of C- or below will require the course to be repeated.

Grade	Description of Work

A	Clearly stands out as excellent performance. Has unusually sharp insights into material and initiates thoughtful questions. Sees many sides of an issue. Articulates well and writes logically and clearly. Integrates ideas previously learned from this and other disciplines. Anticipates next steps in progression of ideas. Example "A" work should be of such nature that it could be put on reserve for all cohort members to review and emulate. The "A" cohort member is, in fact, an example for others to follow.
B	Demonstrates a solid comprehension of the subject matter and always accomplishes all course requirements. Serves as an active participant and listener. Communicates orally and in writing at an acceptable level for the degree program. Work shows intuition and creativity. Example "B" work indicates good quality of performance and is given in recognition for solid work; a "B" should be considered a good grade and awarded to those who submit assignments of quality less than the exemplary work described above.
C	Quality and quantity of work in and out of class is average. Has marginal comprehension, communication skills, or initiative. Requirements of the assignments are addressed at least minimally.
D	Quality and quantity of work is below average. Has minimal comprehension, communication skills, or initiative. Requirements of the assignments are addressed at below acceptable levels.
F	Quality and quantity of work is unacceptable and does not qualify the student to progress to a more advanced level of work.

Course Workshop Summary

Workshop	Devotional*	Discussion*	Journal Assignment*	Assignment*	End-of-Course Survey*	Total Points
Workshop One	1/10	1/25	1/20	2/100		155
Workshop Two	1/10	2/50	1/20	1/50		130
Workshop Three	1/10	2/75	-	2/100		185
Workshop Four	1/10	1/25	-	3/125		160
Workshop Five	1/10	2/75	-	2/75		160
					10	

Workshop Six	1/10	1/25	-	3/175	10 (Extra Credit)	210
Course Totals	**6/60**	**9/275**	**2/40**	**13/625**	**10 (Extra Credit)**	**1000**

* Number of Activities/Sum Point Totals

Course Assignments

Workshop One Outline

Title	Due Dates
1.1 Discussion: A Need for Order	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
1.2 Discussion: Why the Government Needs to Be Involved	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
1.3 Journal Assignment: Economic Implications	Due by the end of the workshop
1.4 Assignment: Crime, Espionage, or War?	Due by the end of the workshop.
1.5 Assignment: U.S. National Security Implications: Essay 1 of 4	Due by the end of the workshop.

* These times are only estimates. Actual assignment completion times will vary.

Workshop Two Outline

Title	Due Dates
2.1 Discussion: Laws and Policies	Initial post due by the end of the fourth day of the wc responses due by the end of the workshop.
2.2 Discussion: History of Cybersecurity Policy	Initial post due by the end of the fourth day of the wc responses due by the end of the workshop.
2.3 Journal Assignment: Development of U.S. Cybersecurity Policy	Due by the end of the workshop

2.4 Discussion: Video Presentation: U.S. Cybersecurity and International Relations, Part 1 of 3	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop.
2.5 Assignment: U.S. National Security Implications: Essay 2 of 4	Due by the end of the workshop.

*These times are only estimates. Actual assignment completion times will vary.

Workshop Three Outline

Title	Due Dates
3.1 Discussion: Peace in Times of Uncertainty	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop.
3.2 Discussion: Economic Espionage	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop.
3.3 Assignment: Incident Response Options Research Paper, Part 1 of 2	Due by the end of the workshop.
3.4 Assignment: U.S. Government Structure and Leads Presentation	Due by the end of the workshop.
3.5 Assignment: Video Presentation: U.S. Cybersecurity and International Relations, Part 2 of 3	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop.

*These times are only estimates. Actual assignment completion times will vary.

Workshop Four Outline

Title	Due Dates
4.1 Discussion: One Body, Many Parts	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop.
4.2 Discussion: What Should Be Secret	Initial post due by the end of the fourth day of the wo responses due by the end of the workshop

	responses due by the end of the workshop.
4.3 Assignment: From Cyber Incident to National Security Incident: Short Essay	Due by the end of the workshop.
4.4 Assignment: Whole of Government Response: Research Paper	Due by the end of the workshop.
4.5 Assignment: National Security Implications: Essay 3 of 4	Due by the end of the workshop.

* These times are only estimates. Actual assignment completion times will vary.

Workshop Five Outline

Title	Due Dates
5.1 Discussion: Alliances for Peace	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
5.2 Discussion: International Organizations	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
5.3 Assignment: Economics and Espionage: Short Essay	Due by the end of the workshop
5.4 Assignment: International View of Cyberwar: Position Paper	Due by the end of the workshop
5.5 Discussion: Video Presentation: U.S. Cybersecurity and International Relations, Part 3 of 3	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.

*These times are only estimates. Actual assignment completion times will vary.

Workshop Six Outline

Title	Due Dates
6.1 Discussion: A Time for War and a Time for Peace	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
6.2 Discussion: War Reference Letter	Initial post due by the end of the fourth day of the wor

6.2 Discussion: What Defines an Act of War via Cyberspace?	Initial post due by the end of the fourth day of the wor responses due by the end of the workshop.
6.3 Assignment: Deterrence versus Response: Short Essay	Due by the end of the workshop.
6.4 Assignment: Current U.S. National and Military Strategy in Cyberspace: Position Paper	Due by the end of the workshop.
6.5 Assignment: National Security Implications: Essay 4 of 4	Due by the end of the workshop.
Survey/Quiz: End-of-Course Survey	Due by the end of the workshop.

*These times are only estimates. Actual assignment completion times will vary.

Course Development Resources

Department of Defense. (2013). Joint publication 3-12 (R): Cyberspace operations. Washington, DC. Retrieved from http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf

Department of Defense. (2015). The national military strategy of the United States of America: The United States Military's contribution to national security. Retrieved from http://www.jcs.mil/Portals/36/Documents/Publications/2015_National_Military_Strategy.pdf

Department of Homeland Security. (2017, December 08). What is critical infrastructure? Retrieved from https://www.dhs.gov/what-critical-infrastructure

Easttom, C. (2016). Computer security fundamentals. Indianapolis, Indiana: Pearson.

Extance, A. (2015). The future of cryptocurrencies: Bitcoin and beyond. Nature, 526(7571), 21–23. doi:10.1038/526021a

Goh, B. (2016). Securing the smart city. Kennedy School Review, 163(2-38).

Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2015). Cybercrime and digital forensics. New York, NY: Routledge.

Huang, A. (2015). Reaching within silk road: The need for a new subpoena power that targets illegal bitcoin transactions. Boston College Law Review, 56(5), 2093–2125.

Indiana Wesleyan University. (n.d.). How to post a video note in a discussion. Retrieved from https://kb.indwes.edu/api/deki/files/5594/Video_Note.pdf?revision=1

Indiana Wesleyan University. (n.d.). How to write an engaging online discussion post. Retrieved from https://media.pearsoncmg.com/pls/in/iwu/brightspace/How_to_Write_an_Engaging_Online_D

Indiana Wesleyan University. (n.d.). OCLS critical evaluation checklist for internet websites. Retrieved from http://www2.indwes.edu/WebEvaluation.html

Indiana Wesleyan University. (2017, July 21). How to post a video note in a discussion. Retrieved from https://kb.indwes.edu/Web/Academic/LMS_(LearningStudio_and_Brightspace)/Student_Guide

Jingguo, W., Gupta, M., & Rao, H. R. (2015). Insider threats in a financial institution: Analysis of attack-proneness of information systems applications. MIS Quarterly, 39(1), 91–112.

Libicki, M. (2016). Cyberspace in peace and war. Annapolis, MD: Naval Institute Press.

NATO. (2018, February 19). Cyber defense. Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm

Schmitt, M. (2013). Tallinn manual on the international law applicable to cyber warfare. New York,