PPOL/PSCI 4396
CYBER POLICY AND NATIONAL SECURITY

Spring 2025

Course Overview

Meetings: Tu/Th 4:00 pm – 5:15 pm
Classroom: FO 1.202
Course website: UTD eLearning

Instructor Information

Name: Marcelo Leal
Email: marcelo.leal@utdallas.edu
Office: GR 3.526
Office hours: Tu 1:30–3:30 pm (or by appointment)

TA Information

Name: Camron Hollis
Email: camron.hollis@utdallas.edu
Office: GR 3.318
Office hours: Th 1–3 pm

COURSE INFORMATION

Description

This course examines the role of cybersecurity in national security, focusing on how nations respond to digital threats. Through case studies, simulations, and discussions, students will explore the technical aspects of cybersecurity, the political dimensions of cyber conflict, and strategies for addressing emerging challenges. Topics include cyber warfare, foreign information operations, critical infrastructure protection, and supply chain security, among others. By the end of the course, students will gain essential tools to analyze cybersecurity threats and their impact on national and global stability.

Learning outcomes

After participating in class, completing the assigned readings, and thinking about course materials, you should be able to achieve the following learning outcomes:

Basic

- *Identify* key actors and events in the cybersecurity field
- *Describe* the basic dynamics of cybersecurity operations
- *Summarize* theoretical concepts used by cybersecurity experts

Intermediate

- *Apply* models and theories to analyze cybersecurity events
- *Compare and contrast* cybersecurity strategies and operations
- *Examine* cybersecurity national policies and international norms

Advanced

- *Evaluate* the strengths and weaknesses of cybersecurity strategies
- *Support* distinct cybersecurity policies with empirical evidence
- *Develop* your own policy solutions to cybersecurity problems

Course materials

Required readings will be available at the course webpage. Course materials will also include videos, podcasts and other forms of information. The following books are good sources of information about cybersecurity, and you can access them online through the UTD library website.

- Dunn Cavelty, Myriam, and Andreas Wenger, eds. *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*. New York: Routledge, 2022.
- Cornish, Paul, ed. *The Oxford Handbook of Cyber Security*. Oxford: Oxford University Press, 2021.
- Reveron, Derek S., and John E. Savage. *Security in the Cyber Age: An Introduction to Policy and Technology*. New York: Cambridge University Press, 2024.
- Van Puyvelde, Damien, and Aaron Franklin Brantly. *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Medford: Polity Press, 2019.
- Whyte, Christopher, and Brian M. Mazanec. *Understanding Cyber Warfare: Politics, Policy and Strategy*. 2nd edition. London: Routledge, 2023.

There are no required books for this course.

GRADING AND ASSESSMENT

Your final grade will be based on the following assignments:

Attendance and Participation	20%
Exams	60%
Cyber Crisis Simulation	15%
Design a Meme	5%

Attendance and Participation

You are expected to attend each class and participate in class discussions. Participation for this course can take several forms, including answering instructor questions, asking clarifying questions on course material, and engaging productively with your peers during group work and class discussion.

Participation is evaluated in two stages: during the first half of the semester, you can earn up to 10 points, and during the second half, you can earn an additional 10 points. This totals a maximum of 20 points for the entire course.

1st Half		2nd Half		Total
10 points	+	10 points	=	20 points

Exams

There will be two exams during the semester. The first exam, scheduled for March 4, will cover all topics discussed up until that date. The second exam, held on May 6, will focus on material covered after Spring break.

Each exam will consist of 30-40 multiple-choice questions and 1-3 open-ended questions. These are open-note exams. Be mindful that only your personal notes are allowed, and these will be inspected by the TA and instructor before the exam.

Exam 1		Exam 2		Total
30 points	+	30 points	=	60 points
March 4		*May 6*		

Both exams will take place during class time. Remote testing is not allowed. Students with ARC accommodations requiring extra time must schedule a separate testing session with the instructor at least two weeks before the exam dates. No make-up exams will be offered, except in cases covered by the excused absence policy.

All materials covered in class or shared on eLearning, except those marked as optional, are subject to the exams. I do not release exams to students, but you can view your exam with me during office hours.

There is no final exam for this course.

Cyber Crisis Simulation

After the first exam, you will participate in an in-class cyber crisis simulation. Active participation in this activity is required. At the end of the simulation, you will write a short report (up to a one-page, single-spaced) discussing key learning points of the simulation, as well as evaluating your own participation and that of your peers. The report must be handed in during class on March 13.

Simulation
15 points

March 6 – 13

Design a Meme

By the end of the semester, you will create an original meme related to cybersecurity. You may use a popular meme template or your own image, but the caption must be entirely your own work. All content must be appropriate for an academic setting.

Along with the meme, you will write a brief explanation (no more than one single-spaced page, not including the meme) discussing how your meme relates to cybersecurity concepts, challenges, or policies. The assignment is due on eLearning by May 8 at noon. On that same day, students will present their memes to the whole class during our last meeting.

Design a Meme
5 points

May 8

Grade Scale

For your final letter grade, I round the final numerical grade up to the next highest whole number if it is greater than or equal to 0.5 (e.g., 86.5 becomes 87). Individual assignment grades are not rounded. Final letter grades are determined as follows:

A+	100 – 97	B+	89 – 87	C+	79 – 77	D+	69 – 67	**F**	59 or less
A	96 – 94	B	86 – 84	C	76 – 74	D	66 – 64		
A-	93 – 90	B-	83 – 80	C-	73 – 70	D-	63 – 60		

COURSE POLICIES

Communication

If I need to contact you for any reason, I will use your UTD email address. Please make sure you check your mailbox regularly throughout the semester and follow proper e-mail etiquette. I typically respond to emails within one-two business days and expect you will do the same. I respond to emails Monday-Friday from 8 am – 5 pm.

Electronic devices

To ensure a focused learning environment, cell phone use is prohibited during class. Please silence and store your phone before entering the classroom. Laptops and tablets are allowed for note-taking and approved class activities only. Using devices for unrelated activities (e.g., social media, messaging, gaming) is prohibited and may result in a ban on all electronic devices during class.

Class recordings

The instructor may record meetings class course, with recordings made available to all registered students to supplement learning. Any other use of recordings requires the consent of identifiable students unless permitted by law. Students must follow University policies and protect passwords for accessing recorded lectures. Unless the AccessAbility Resource Center has approved the student to record the instruction, students are expressly prohibited from recording any part of this course. Recordings may not be published, reproduced, or shared with those not in the class, or uploaded to other online environments except to implement an approved accommodation. Failure to comply with these University requirements is a violation of the Student Code of Conduct.

Grade disputes

You can discuss your assignment grade with your TA starting 24 hours after it is returned. Submit your questions and justification for a grade change in writing (email preferred) before the meeting. Note that grades can go up or down upon review. Grade disputes must be submitted within seven days of receiving your grade. If the dispute is unresolved after the TA's review, the instructor will review it. The same process applies: email your justification in advance and come prepared to discuss it.

Late work

Late work will be accepted up to 24 hours after the deadline, but they will be subject to a 10-percentage penalty. After that, I will not accept any assignment without prior, written authorization from your TA or me, except in cases of clear-cut family, personal, or medical emergency. If you have a problem meeting any deadline, please discuss this with the TA or me well before the due date or provide documentation of the problem afterwards.

Extra credit

Extra credit is not offered on an individual basis. Over the course of the semester, I reserve the right to make extra credit opportunities available to all students equally, in the interest of fairness. Please do not request additional assignments for extra credit.

Excused absences

Excused absences are limited to observed religious holidays (per UTD policy), military service, official UTD events (e.g., athletics, debate, Moot Court), COVID-related exposure, or serious illness, provided you notify me in advance via email or in person. Documentation may be requested at the discretion of the instructor. Excused absences are not granted for work, vacations, doctor's appointments, family events, or other personal matters. You do not need to inform me of such absences. One unexcused absence will not significantly affect your grade as long as it is not a test day and you submit assignments due that day before the deadline. I will not schedule exams early or late for individual students' personal issues.

UTD POLICIES AND RESOURCES

Accommodations for Students with Disabilities

The University of Texas at Dallas is committed to providing reasonable accommodations for all persons with disabilities. The syllabus is available in alternate formats upon request. If you are seeking classroom accommodations under the Americans with Disabilities Act (2008), you are required to register with the AccessAbility Resource Center (ARC), located in the Administration Building, Suite 2.224. They can be reached by email, calling 972-

883-2098, or at their website. To receive academic accommodations for this class, please register and request services by completing the Request for Services form with the proper documentation and meeting with the Director of ARC at the beginning of the semester.

Academic Support Resources
Please visit the Academic Support Resources page to view the University's academic support resources for all students.

UT Dallas Syllabus Policies and Procedures
Please visit the Syllabus Policies page to view the University's policies and procedures segment of the course syllabus.

COURSE SCHEDULE

The schedule is subject to change. Any changes will be communicated to students in advance through their UTD email and in class. You must read only the required (Req) readings. The optional readings (Opt) are, as the name says, optional.

Week 1	January 21 & 23

Cybersecurity: Security from What, for Whom, and by What Means?

Req Syllabus

Req Dunn Cavelty, Myriam, and Andreas Wenger. "Introduction." In *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, 1-13 New York: Routledge, 2022.

Opt Dunn Cavelty, Myriam, and Andreas Wenger. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41, no. 1 (2020): 5–32.

Week 2	January 28 & 30

Vulnerabilities and Threats in Cyberspace: Technical Aspects

Req Miller, Chris. "Introduction." In *Chip War: The Fight for the World's Most Critical Technology*, 11–18. New York: Simon and Schuster, 2022.

Req Sherman, Justin. "Cybersecurity under the Ocean: Submarine Cables and US National Security." Aegis Series Paper. Hoover Institution, January 18, 2023.

https://www.lawfareblog.com/cybersecurity-under-ocean-submarine-cables-and-us-national-security.

Opt Brock, Joe. "U.S. and China Wage War beneath the Waves - over Internet Cables." News. Reuters, March 24, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-cables/.

Week 3	February 4 & 6

Vulnerabilities and Threats in Cyberspace: The Human Dimension

Req Lin, Herbert, and Jaclyn Kerr. "On Cyber-Enabled Information Warfare and Information Operations." In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish, 251–272. Oxford University Press, 2021.

Req Wilde, Gavin. "From Panic to Policy: The Limits of Foreign Propaganda and the Foundations of an Effective Response." *Texas National Security Review* 7, no. 2 (2024): 42–55.

Opt Lewis-Kraus, Gideon. "How Harmful Is Social Media?" The New Yorker, June 3, 2022. https://www.newyorker.com/culture/annals-of-inquiry/we-know-less-about-social-media-than-we-think.

Week 4	February 11 & 13

Cyber War is Coming: Threat Inflation and National Security

Req Damien Van Puyvelde, and Aaron F. Brantly. "Cyber war." In *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, 90–101. Cambridge, UK: Polity, 2019.

Req Lindsay, Jon R. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22, no. 3 (2013): 365–404.

Opt Slayton, Rebecca. "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment." *International Security* 41, no. 3 (January 2017): 72–109.

Week 5	February 18 & 20

Crisis Bargaining in the Gray Zone: The Logics of Coercion and Deterrence

Req Borghard, Erica D., and Shawn W. Lonergan. "The Logic of Coercion in Cyberspace." *Security Studies* 26, no. 3 (2017): 452-481.

Req Valeriano, Brandon. “Introduction: Are Cyber Strategies Coercive?” In *Cyber Strategy: The Evolving Character of Power and Coercion*, edited by Brandon Valeriano, Benjamin Jensen, and Ryan C. Maness, 1–21. Oxford University Press, 2018.

Opt Cornish, Paul. “The Deterrence and Prevention of Cyber Conflict.” In *The Oxford Handbook of Cyber Security*, edited by Paul Cornish, 1st ed., 273–294. Oxford University Press, 2021.

Week 6	February 25 & 27

Cyber Conflict as an Intelligence Contest: Covert Action and Information Control

Req Rovner, Joshua. “What Is an Intelligence Contest?” *Texas National Security Review* 3, no. 4 (2020): 114–120.

Req Kostyuk, Nadiya, and Erik Gartzke. “Why Cyber Dogs Have Yet to Bark Loudly in Russia’s Invasion of Ukraine.” *Texas National Security Review* 5, no. 3 (2022): 113–126.

Opt “Policy Roundtable: Cyber Conflict as an Intelligence Contest,” *Texas National Security Review*, June 2, 2020, https://tnsr.org/roundtable/policy-roundtable-cyber-conflict-as-an-intelligence-contest/.

Week 7	March 4 & 6

March 4: Exam 1 (in person)

March 6: Cyber Crisis Simulation (in person)

Week 8	March 11 & 13

March 11: Cyber Crisis Simulation (in person)

March 13: Cyber Crisis Simulation Report due in class

Week 9	SPRING BREAK

Week 10	March 25 & 27

U.S. Cybersecurity Strategy: From Restraint to Defend Forward

Req United States Government. *National Cybersecurity Strategy*. Washington, D.C.: The White House, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

Req Vićić, Jelena, and Gregory H. Winger. "What the Defense Department's Cyber Strategy Says About Cyber Conflict." Lawfare, October 19, 2023. https://www.lawfaremedia.org/article/what-the-defense-department-s-cyber-strategy-says-about-cyber-conflict.

Opt Healey, Jason. "Twenty-Five Years of White House Cyber Policies." Lawfare, June 2, 2023. https://www.lawfaremedia.org/article/twenty-five-years-of-white-house-cyber-policies.

Week 11 April 1 & 3

U.S. Cybersecurity Policies: A Whole-of-Nation Effort

Req Atkins, Sean, and Chappell Lawson. "An Improvised Patchwork: Success and Failure in Cybersecurity Policy for Critical Infrastructure." *Public Administration Review* 81, no. 5 (2021): 847–61.

Req Bate, Laura. "The Cyber Workforce Gap: A National Security Liability?" War on the Rocks, May 17, 2017. https://warontherocks.com/2017/05/the-cyber-workforce-gap-a-national-security-liability/.

Opt Clark-Ginsberg, Aaron, and Rebecca Slayton. "Regulating Risks Within Complex Sociotechnical Systems: Evidence from Critical Infrastructure Cybersecurity Standards." *Science and Public Policy* 46, no. 3 (2019): 339–46.

Week 12 April 8 & 10

Cybersecurity Strategies beyond the U.S.: Perspectives from Allies and Rivals

Req Jacobsen, Jeppe T. "Cyber Offense in NATO: Challenges and Opportunities." *International Affairs* 97, no. 3 (2021): 703–720.

Req Grzegorzewski, Mark, and Christopher Marsh. "A Strategic Cyberspace Overview: Russia and China." In *Great Power Cyber Competition: Competing and Winning in the Information Environment*, edited by David V. Gioe and Margaret W. Smith, 6–24. London: Routledge, 2023.

Opt Broeders, Dennis, Fabio Cristiano, and Monica Kaminska. “In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions.” *JCMS: Journal of Common Market Studies* 61, no. 5 (2023): 1261–80.

Week 13	April 15 & 17

Global Cybersecurity Governance: (Re)Building International Norms

Req Nye, Joseph S. “The End of Cyber-Anarchy? How to Build a New Digital Order.” *Foreign Affairs*, December 14, 2021. https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy.

Req Sukumar, Arun, Dennis Broeders, and Monica Kello. “The Pervasive Informality of the International Cybersecurity Regime: Geopolitics, Non-State Actors and Diplomacy.” *Contemporary Security Policy* 45, no. 1 (2024): 7–44.

Opt Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” *American Journal of International Law* 110, no. 3 (2016): 425–479.

Week 14	April 22 & 24

Governance Beyond the Battlefield: The Fight Over Who Controls the Internet

Req Carr, Madeline. “Power Plays in Global Internet Governance.” Millennium: *Journal of International Studies* 43, no. 2 (2015): 640–59.

Req Bradford, Anu. “Introduction.” In *Digital Empires: The Global Battle to Regulate Technology*, 1-29. Oxford University Press, 2023.

Opt Denardis, Laura. “The Internet Governance Oxymoron.” In *The Global War for Internet Governance*, 1-32. Yale University Press, 2014.

Week 15	April 29 & May 1

Planning for an Uncertain Future: Artificial Intelligence and Cybersecurity

Req Henry A. Kissinger, Eric Schmidt and Craig Mundie, "War and Peace in the Age of Artificial Intelligence." Foreign Affairs, November 18, 2024. https://www.foreignaffairs.com/united-states/war-and-peace-age-artificial-intelligence.

Req Jensen, Benjamin M, Christopher Whyte, and Scott Cuomo. “Algorithms at War: The Promise, Peril, and Limits of Artificial Intelligence.” *International Studies Review* 22, no. 3 (2020): 526–50.

Opt “Policy Roundtable: Artificial Intelligence and International Security,” *Texas National Security Review*, June 2, 2020, https://tnsr.org/roundtable/policy-roundtable-artificial-intelligence-and-international-security/.

Week 16	May 6 & 8

- May 6: Exam 2 (in class)
- May 8: Design a Meme Presentations (in class)
- May 8, at noon: Submit Design a Meme assignment (on eLearning)