Course Syllabus

INTL 4666E: Politics of Cyber Security

Summer 2026

Pre-requisites: INTL 3200/3200E/3200H or INTL 3300/3300E/3300H

Course Meeting Times

Class Meeting Time: Online

Class Meeting Mode: Primarily asynchronous

Instructor & TA Information

Instructor: Dr. Rongbin Han

Email: email via eLC

Office Hours: TBA

Website: https://spia.uga.edu/faculty-member/rongbin-han/

The best way to contact the instructor is via email. Emails are normally returned within 24 hours during working days. Please reach out if you do not receive a response beyond the timeframe.

Course Description & Details

An introduction to the basics of cyber security, with a focus on its humanistic, social, and political implications. Exploration of the empirical and normative themes that relate cyber security to our students as members of a community, a society, and a nation.

Course-level Learning Outcomes

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

- recall and apply key concepts in international affairs (e.g., the international system, actors in the international system, the principles of sovereignty and anarchy).
- compare and contrast various political systems and consider their advantages and disadvantages from the perspective of different societal actors.
- explain, critique, and apply the major theoretical approaches and models used within international relations and comparative politics.
- practice evaluating the causes and effects of historical and contemporary global events, by choosing and applying appropriate theoretical models, interpreting and contextualizing past research findings, and/or analyzing empirical data (qualitative or quantitative).

- locate sources of data and evaluate their credibility and their appropriateness for testing a given theory or hypothesis.
- articulate opinions on certain global issues, informed by the application of theoretical models, research findings, and/or empirical data (qualitative or quantitative).
- express their opinions on certain global issues through formal writing assignments and have the opportunity to revise and refine their writing in response to feedback from the instructor.
- identify the key components of social science research.
- appreciate and analyze policy interdependence--that is, how the choices that one actor or group of actors make (e.g., citizens, firms, countries) affect the lives and decisions of other actors or groups of actors.

COURSE TOPICS

- Introduction
- Fundamentals about the Cyber Society
- The Sources of Cyber Threats: A General Introduction
- Cyber Security and Individuals
- Cyber Security and Organizations
- Cyber Security and Nations
- Cyber Security and Democracy
- Cyber Security and the Future of Humanity

Required Course materials

Most course materials are either available online or will be made available on ELC or through UGA Library. Notify the instructor if you cannot access course materials.

Assessment and Grading

Course Assignments & Requirements	Due Date	Portion of Final Grade	Submission Information
Reading Response	Rolling basis	15%	eLC/discussion forum
AI Trial Report	May 22	15%	eLC/discussion forum
Video Recommendation	May 27	10%	eLC/discussion forum
Final Think Piece	June 3	30%	eLC/Assignment
Final Quiz	June 3	10%	eLC/Quiz
Participation	Throughout	20%	eLC

See eLC for more information about each course requirement.

Exam Information

The final quiz will be conducted online. It will be made available for 24 hours. Students have 15 minutes to complete once they start the quiz. The quiz requires Respondus LockDown Browser.

Participation Information

Participation in this course will take place primarily asynchronously. Students are expected to (1) do ALL the readings and the course modules and (2) engage in discussion via ELC for each module (by directly responding to the discussion questions and/or reacting to other students, initiating new discussion threads. The grade will be based on the frequency, quality, and effectiveness of participation; to receive a grade of B or higher for this item alone, students need to respond to at least 14 of all the discussion questions with decent quality. Students are also encouraged to attend virtual office hours. In total, participation will contribute 20% to your final grade.

Missed Exams, Late Assignments, & Re-grading Requests

Please submit your assignments timely. Late assignments will be accepted **before the Maymester ends**, though for fairness, it will result in a penalty of one third of a letter grade per day. For questions about your grade, report to the instructor **within one week from the time you receive the grade**, with a written appeal explaining why you think your grade should be changed. Please bear in mind that the regrading process may end up with higher, lower or no change in your grade.

Final Grades

A 93-100	A- 90-92.99	B+ 87-89.99	B 83-86.99	B- 80-82.99
C+ 77-79.99	C 73-76.99	C- 70-72.99	D 60-69.99	F 0-59.99

Course Statements & Policies

UGA Honor Code

As a University of Georgia student, you agree to abide by the University's academic honesty policy, "A Culture of Honesty," and the Student Honor Code. All academic work must meet the standards described in "A Culture of Honesty" found at: honesty.uga.edu.

Accommodation for Disabilities

If you plan to request accommodations for a disability, please register with the *Accessibility & Testing*. They can be reached by visiting Clark Howell Hall, calling 706-542-8719 (voice) or 706-542-8778 (TTY), or by visiting https://accessibility.uga.edu/.

ATTENDANCE & PARTICIPATION POLICY

This is an online course. Therefore, no attendance will be taken. However, your participation will be crucial for the successful completion of this course. You are expected to do all the readings and course modules and actively participate in online discussions. You are encouraged to attend virtual office hours.

USE OF AI IN THIS COURSE

UGA's policy is that the use of AI for coursework is not permitted unless explicitly authorized by me (your course instructor) ahead of time. In this class, ***use of GAI tools should be limited to providing support as you develop your thinking and knowledge base.*** In addition, there are some general rules to follow:

- You may not represent output generated by a GAI tool as your own work. Any such use of GAI output must be appropriately cited or disclosed, including quotation marks and in-line citations for direct quotes. Including anything you did not write in your assignment without proper citation will be treated as an academic misconduct case. Suspected unauthorized assistance, plagiarism, or other violations of UGA's "A Culture of Honesty," will be reported to the Office of Academic Honesty. For full details on how to properly cite AI-generated work, please see the APA Style article, How to Cite ChatGPT, for instance
- If you are unsure where the line is between collaborating with GAI and copying from GAI, I recommend that you do not have your assignment and the GAI tool open on your device at the same time. Instead, take notes in your own words while you interact with the GAI tool, then use your notes to remind you of what you've learned and to inform your work. Never copy output from GAI tools into your assignment. Instead, use your interaction with the tool as a learning experience, then close the interaction down, open your assignment, and let your assignment reflect your improved understanding. (Sidenote: This advice extends to AI assistants that are directly integrated into a composition environment or grammar modulation tool.)
- Finally, GAI is highly vulnerable to inaccuracy and bias. You should assume GAI output is wrong unless you either know the answer or can verify it with another source. It is your responsibility to assess the validity and applicability of any GAI output used.

WELL-BEING RESOURCES

UGA Well-being Resources promote student success by cultivating a culture that supports a more active, healthy, and engaged student community.

Anyone needing assistance is encouraged to contact Student Care & Outreach (SCO) in the Division of Student Affairs at 706-542-8479 or visit sco.uga.edu. Student Care & Outreach helps students navigate difficult circumstances by connecting them with the most appropriate resources or services. They also administer the Embark@UGA program which supports students experiencing, or who have experienced, homelessness, foster care, or housing insecurity.

UGA provides both clinical and non-clinical options to support student well-being and mental health, any time, any place. Whether on campus, or studying from home or abroad, UGA Well-being Resources are here to help.

- Well-being Resources: well-being.uga.edu

- Student Care and Outreach: sco.uga.edu
- University Health Center: healthcenter.uga.edu
- Counseling and Psychiatric Services: caps.uga.edu or CAPS 24/7 crisis support at 706-542-2273
- Health Promotion/ Fontaine Center: healthpromotion.uga.edu
- Accessibility & Testing: accessibility.uga.edu

Additional information, including free digital well-being resources, can be accessed through the UGA app or by visiting well-being.uga.edu.

STUDENT SUCCESS RESOURCES

The Office for Student Success and Achievement (OSSA) empowers students to achieve success throughout their academic journey. Through free peer tutoring, academic coaching, UNIV student success courses, Bulldog Basics, and first-generation student support, we promote well-being, student learning, and community building. To connect with OSSA, email *ossa@uga.edu*, call (706) 542-0163, or visit Milledge Hall (near Reed Hall and Sanford Stadium).

DISCLAIMER

The course syllabus is a general plan for the course; deviations announced to the class by the instructor may be necessary.

Course Schedule & Activities

1: Introduction
* The Syllabus

Suggested:
* Scott Malcomson, “The New Cybernormal,” *Carnegie Reporter* (June 7, 2018).
* Robert Ramirez and Nazli Choucri, ““Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review,” *IEEE Access*, 4 (March 2016): 2216-43.

2: Fundamentals about the Cyber Society
* Wikipedia, “Computer Architecture.”
* Wikipedia, “Internet.”
* Stephen Crocker, “How the Internet Got Its Rules,” New York Times (April 7, 2009).
* Tim Berners-Lee, “Long Live the Web: A Call for Continued Open Standards and Neutrality,” Scientific American Magazine (December 2010), 80-85.
* ICANN, “Beginner's Guide to Internet Protocol (IP) Addresses.”
* John Biggs, “A Tiny Computer Attracts a Million Tinkerers,” New York Times (January 31, 2013).
* Joshua Sperber, “Yelp and Labor Discipline: How the Internet Works for Capitalism,” New Labor Forum. 23(2):68-74.
* Catherine Rampell, “Our politicians have no idea how the Internet works,” The Washington Post (August 21, 2018).
* John Boitnott, “Why Silicon Valley Income Inequality is Just a Preview of What’s to Come for the Rest of the U.S.,” Inc. (October 18, 2018).

Suggested:
* Khan Academy, “Internet 101.” [Strongly recommended]
* Carol Hand, *How the Internet Changed History* (Minneapolis, MN: Abdo Publishing, 2016), eBook available via UGA library

3: Sources of Cyber Threats
* Tarah Wheeler, “In Cyberwar, There Are No Rules,” Foreign Policy (Fall 2018): 36-41.
* Symantec, “Internet Security Threat Report 2019,” Symantec Corporation, pp. 14-58.
* CSIS, “Significant Cyber Incidents Since 2006.”
* Daniel R. Coats, “Worldwide Threat Assessment of the US Intelligence Community,” State for the Record at the Senate Select Committee on Intelligence, January 29, 2019.
* Peter W. Singer, “The "Oceans 11" of Cyber Strikes,” Brookings Institute (May 21, 2012).
* Joshuah Bearman and Tomer Hanuka, “The Rise of Fall of Silk Road (Part I),” and "The Rise of Fall of Silk Road (Part II)," Wired (May 2015).
* Colin Lecher, “How Amazon Automatically Tracks and Fires Warehouse Workers for ‘Productivity’,” The Verge (April 25, 2019).
* Adam Bannister, "Microsoft falls prey to SolarWinds supply chain cyber-attacks," The Daily Swig (December 18, 2020).

4: Privacy & Personal Data Security

* Lily Hay Newman, “The Wired Guide to Data Breaches,” Wired (December 7, 2018).
* Matt Day, Giles Turner, and Natalia Drozdiak, “Thousands of Amazon Workers Listen to Alexa Users' Conversations,” Time (April 11, 2019).
* Andre Mayer and Michael Pereira, “Digital surveillance: How you're being tracked every day,” CBC News.
* Consumer Reports, “Consumer Reports Launches Digital Standard, Begins Evaluating Products, Services for Privacy and Data Security,” Consumer Reports (March 6, 2017).
* Ewen MacAskill and Alex Hern, “Edward Snowden: ‘The People Are Still Powerless, But Now They’re Aware,” The Guardian (June 4, 2018).
* Byron Tau, "U.S. Government Contractor Embedded Software in Apps to Track Phones," Wall Street Journal (August 7, 2020).

Suggested:

* John Oliver, “Government Surveillance: Last Week Tonight with John Oliver,” HBO.

5: Living Networked

Social Media Pressure

* Jessica Brown, “Is Social Media Bad for You? The Evidence and the Unknowns,” BBC (January 5, 2018).
* Association for Psychological Science, “Social Media ‘Likes’ Impact Teens’ Brains and Behavior.” [If interested, check out the original article: Lauren Sherman et al, “The Power of the Like in Adolescence: Effects of Peer Influence on Neural and Behavioral Responses to Social Media,” Psychological Science 27:7 (2016): 1027-1035.]
* Rebecca Greenfield, “How Social Pressure Gets Facebook Friends to Vote,” The Atlantic (Nov. 6, 2012).
* Erin Brodwin, “What Psychology Actually Says about the Tragically Social Media Obsessed Society in ‘Black Mirror’,” Business Insider (Oct. 26, 2016).
* Paul Miller, “I’m still here: back online after a year without the internet,” The Verge (May 1, 2013).

Cyberbullying & Online Harassment

* StopBullying, “Cyberbully.”
* Cybersecurity & Infrastructure Security Agency, “CISA: Dealing with Cyberbullies,” (February 01, 2021).

In the Name of Love

* Tasha Robinson, “Black Mirror’s Arkangel Misses Out on So Many Story Opportunities,” *The Verge* (Jan. 8, 2018).

Suggested:

* John Oliver, “Online Harassment: Last Week Tonight with John Oliver,” HBO, June 21, 2015.
* Black Mirror (Season 3 Episode 1): NoseDive
* Black Mirror (Season 4 Episode 2): Arkangel

6: Movie Day

TERMS AND CONDITIONS MAY APPLY (2013)

7: Cyber Security & Corporations

* David E. Sanger, “Tech Firms Sign ‘Digital Geneva Accord’ Not to Aid Governments in Cyberwar,” New York Times (April 17, 2018).
* Lara Seligman, “Why the Military Must Learn to Love Silicon Valley,” Foreign Policy, no. 230 (Fall 2018): 50-53.
* Neri Zilber, “Hackers for Hire,” Foreign Policy, no. 230 (Fall 2018): 61-64.
* Mark Seal, “Sony Under Siege,” Vanity Fair 57:3 (March 2015).
* Russell Brandom, “Wikileaks Has Published the Complete Sony Leaks in A Searchable Database,” The Verge (April 16, 2015).
* Craig Timberg, Elizabeth Dwoskin, and Brian Fung, “Equifax breach hits credit data of millions,” Washington Post (September 8, 2017).
* Rachel Abrams, “Target to Pay $18.5 Million to 47 States in Security Breach Settlement,” New York Times (May 24, 2017).

Also: quickly re-read:

* Symantec, "Internet Security Threat Report 2019," Symantec Corporation, pp. 14-58.
* CSIS, “Significant Cyber Incidents Since 2006.”

Suggested:

* Brad Smith, “34 Companies Stand Up for Cybersecurity with a Tech Accord,” Microsoft Blog (April 17, 2018).
* Oliver Burkeman, "IBM 'dealt directly with Holocaust organisers'," The Guardian (March 29, 2002).
* More technical details regarding the Target hack, see Xiaokui Shu et al, “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned."

Also SUGGESTED: THE DEFENDERS (2018). Note this is not the Marvel’s movie.

8: Movie Day

THE SOCIAL DILEMMA (2020)

9: Regulation Challenges

* John Perry Barlow, “A Declaration of the Independence of Cyberspace,” Electronic Frontier Foundation (February 8, 1996).
* Milton L. Mueller, Network and States: The Global Politics of Internet Governance (MIT Press, 2010), Chapter 1.
* Joseph S. Nye, Jr. “The Regime Complex for Managing Global Cyber Activities,” Global Commission on Internet Governance (May 2014).
* Damian Paletta, “Cyberweapon Deal Unravels,” Wall Street Journal (Oct. 16 2015).
* Jeff Brueggeman, “The Voice of Business: Why internet governance needs strengthening,” The Guardian (17 October 2012).
* Robert Kuttner, "How to Regulate Facebook," Huffpost (March 25, 2018).

* Brian Barrett, “What Would Regulating Facebook Look Like,” Wired (March 21, 2018).
* Gideon Lichfield, “Facebook’s ex security boss: Asking Big Tech to police hate speech is ‘a dangerous path’” MIT Technology Review (October 23, 2018).
* Daniel Araya, “Huawei’s 5G Dominance in the Post-American World,” Forbes (April 5, 2019).

10: National Security & Cyberwarfare

* Herbert Lin and Amy Zegart, “Introduction,” in Herbert Lin and Amy Zegart eds. Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations (Brookings Institution Press, 2019), 1-17.
* Benjamin Jenson and Brandon Valeriano, “U.S. Military Steps up Cyberwarfare Effort,” The Conversation (March 12, 2019).
* Jon Lindsay, “Stuxnet and the Limits of Cyber Warfare,” Security Studies 22:3 (2013): 365-404.
* James Andrew Lewis, “Five Myths about Chinese Hackers,” The Washington Post (March 22, 2013).
* Jack Goldsmith, “Why the USG Complaints Against Chinese Economic Cyber-Snooping Are So Weak,” Lawfare (March 25, 2013).
* Liam Stack, Nick Cumming-Bruce and Madeleine Kruhly, "How Julian Assange and Wikileaks Became Targets of the U.S. Government," New York Times (April 11, 2019).
* Scott Shane, Nicole Perlroth and David E. Sanger, “Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core,” New York Times (November 12, 2017).

Suggested (assigned previously):

* CSIS, “Significant Cyber Incidents Since 2006.”

11: Cyber Terrorism

Gabriel Weimann, Terrorism in Cyberspace: The Next Generation (Columbia University Press, 2015), pp. 15-45.
* Peter W. Singer, “The Cyber Terror Bogeyman,” Brookings Institute (November 1, 2012).
* Paul Tassi, "How ISIS Terrorist May Have Used PlayStation 4 To Discuss And Plan Attacks [Updated]," Forbes (November 14, 2015).
* Bruce Hoffman, “How Serious is White Nationalist Terrorism,” Council on Foreign Relations (March 29, 2019).

Suggested:

* John Cassidy, "It’s Time to Confront the Threat of Right-Wing Terrorism," The New Yorker (March 16, 2019).
* Woodrow Wilson Center, “Terrorism in Cyberspace: The Next Generation,” YouTube (June 18, 2015).
* Keiran Hardy and George Williams, “What is ‘Cyberterrorism’? Computer and Internet Technology in Legal Definitions of Terrorism,” in Thomas Chen, Lee Jarvis, and Stuart Macdonald eds. Cyberterrorism: Understanding, Assessment, and Response (Springer, 2014), 1-24.

12: Digital Authoritarianism (China as an Example)

* Rongbin Han, From empowering Internet to digital dominance: The past, present, and future of cyber politics in China. *Communication and the Public*, *9*:4(2024): 382-391.
* Min Jiang, “The Business and Politics of Search Engines: A Comparative Study of Baidu and Google’s Search Results of Internet Events in China,” New Media & Society 16:2 (2014): 212–33.
* Genia Kostka, “China’s social credit systems and public opinion: Explaining high levels of approval,” *New Media & Society*, *21*:7 (2019): 1565-1593.
* Zhou Jiaquan, “Drones, facial recognition and a social credit system: 10 ways China watches its citizens,” South China Morning Post (August 4, 2018).
* BBC, “Chinese man caught by facial recognition at pop concert,” BBC (April 13, 2018).
* Amy Hawkins, “The Odd Reality of Life under China’s Orwellian Propaganda App,” Wired UK (April 16, 2019).
* Andy Greenberg, "Does Covid-19 Contact Tracing Pose a Privacy Risk? Your Questions, Answered," Wired (April 17, 2020).

Suggested:
Margaret E. Roberts, *Censored: Distraction and Diversion Inside China’s Great Firewall* (Princeton University Press, 2018).
Rongbin Han, *Contesting Cyberspace in China: Online Expression and Authoritarian Resilience* (Columbia University Press, 2018).

13: Digital Challenges toward Democracy
* Kofi Annan, “How IT Threatens Democracy,” Project Syndicate (Feb. 16, 2018).
* Ruth E. Appel et al., "How deceptive online networks reached millions in the US 2020 elections," *Nature Human Behaviour* (2026). https://doi.org/10.1038/s41562-026-02435-2.
* Keir Giles, “Countering Russian Information Operations in the Age of Social Media,” Council on Foreign Relations (November 21, 2017).
* Nathaniel Persily, “Can Democracy Survive the Internet?” Journal of Democracy, 28:2 (2017), 63-76.
* Samantha Bradshaw and Philip Howard, “Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation,” Oxford Internet Institute (2018).
* Laurie Chen, "Overreaction to China threat could turn into McCarthyite Red Scare, says former US official," South China Morning Post (March 31, 2019).
* Alex Hern, “Cambridge Analytica: How Did It Turn Clicks into Votes,” Guardian (May 6, 2018).
* Issie Lapowsky, "How Bots Broke the FCC's Public Comment System," Wired (November 28, 2017).
* David Lazer et al., “The Science of Fake News,” Science 359 (6380): 1094-1096.
* Lorenzo Franceschi-Bicchierai and Riccardo Coluccini, “Researchers Find Google Play Store Apps Were Actually Government Malware,” Motherboard (March 29, 2019).
* Adam Rawnsley, "Right-Wing Media Outlets Duped by a Middle East Propaganda Campaign," The Daily Beast (June 7, 2020).
* Peter Kafka, "Obama: The internet is 'the single biggest threat to our democracy'," Vox (November 16, 2020).
Suggested:
Helmus et al, Russian Social Media Influence (Rand Corporation, 2018).

14: The Future of Humanity

* Steven Melendez, “Can New Forensic Tech Win War On AI-Generated Fake Images?" *Fast Company* (April 4, 2018).
* Samantha Cole, “There is No Tech Solution to Deepfakes,” *Motherboard* (August 14, 2018).
* David Souter, “Inside the Information Society: Permissionless innovation and the precautionary principle,” Association for Progressive Communications (April 2, 2018).
* Daniel Kokotajlo, Scott Alexander, Thomas Larsen, Eli Lifland, and Romeo Dean, AI 2027 (April 3rd, 2025).
* Jake Swearingen, “A.I. Is Flying Drones (Very, Very Slowly),” *The New York Times* (March 26, 2019).
* Chris Stokel-Walker, “DeepMind AI thrashes human professionals at video game StarCraft II,” *New Scientist* (January 24, 2019).
* Peter Holley, “Soon, the most beautiful people in the world may no longer be human,” *The Washington Post* (August 8, 2018).
* Mike Brown, “Elon Musk Reveals the One Question He Would Ask a Human-Level A.I.,” *Inverse* (April 15, 2019).
* John Naughton, “‘The Goal is to Automate Us’: Welcome to the Age of Surveillance Capitalism,” Guardian (January 20, 2019).

***Suggested*:**

* Craig Silverman, “How to Spot A Deepfake Like the Barack Obama–Jordan Peele Video,” *BuzzFeed* (April 17, 2018).
* Shoshana Zuboff and Naomi Klein, “The Rise of Surveillance Capitalism,” *The Intercept* (March 1, 2019).

15: Movie Day/Reflection Day

Enemy of the State (1998), The Matrix (1999) or **Ex Machina (2014)**
Also recommended:
The Matrix Reloaded
The Matrix Revolutions
Person of Interest