INTL 4666E Politics of Cyber Security

Dr. Rongbin Han
<hanr@uga.edu>
University of Georgia

***** Subject to Updates *****

Course Overview and Objectives

Cyber security has become an increasingly critical component of public life today. As a non-traditional security issue, it now affects every one of us as individuals as well as members of a community, a society, and a nation. Moreover, ongoing debates such as those surrounding the Facebook data crisis and foreign influences over the past U.S. presidential election manifest that cyber security is an issue that may jeopardize the liberal democratic institutions and values. This online course will introduce to students the basics about cyber security not from the technical or managerial perspective, but from the humanistic, social, and political angles. There are three primary objectives: (1) By examining cyber security issues from a socio-political perspective, the course hopes to generate awareness among students about the implications of technological development and the future of human society as a whole; (2) By surveying the potential socio-economic and political risks of our networked society from a broad perspective, the course intends to foster a humanistic, societal, and political understanding of cyber security, which in turn prepares students to engage the issue from less technological, but more political and policy points of view; and (3) By preparing students to engage cyber security issues from the political and policy perspectives, the course helps students to develop the ability to communicate across the divide between technological and policy communities.

Accessing Course

Course materials will be hosted primarily on eLC, though I will make use of other online tools for the purpose of communicate with you. And precisely because of the online nature of this course, I'd issue the following warning message:

> ***If you are traveling, make sure that you have sufficient Internet access time and unfettered access to the course site hosted on eLC and relevant services.***

You can access the readings by directly clicking the links on the syllabus. But if the URLs do not work, you should be able to find most readings in the Content/Reading folder. Get in touch with the instructor if you still have difficulty.

Virtual Class Meeting or Office Hour

I will be hosting virtual daily virtual class meeting or office hour sessions between 10:30-11:30 (EST) using **Collaborate Ultra**. You can access it via ELC. I am also happy to use ELC's Chat function, provided that you need it and I am not meeting someone else. Please familiarize yourself with such functions. If you need to chat with me privately, or if you want to meet me in person in Athens, we'll need to set up appointments, too.

Final Grade Ranges:

	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 Requirements and Grading Criteria

Assignments

1. Reading response *(10%)*: Write one response paper (3-4 pages, double spaced) based on the assigned readings for the day of your choice (movie days excluded). The response may take a variety of forms, but should include basic ideas and arguments of the readings, as well as (and more importantly) your own questions, comments, and critical reflections. Feel free to draw on materials outside assigned readings.
2. Reflection on living connected *(10%)* : Write a short piece documenting the (potential) scenarios in which you cut yourself off the Internet entirely for one day, one week, and one month respectively. How that would affect (or not affect) your life? Detail the ways in which your life (every aspect) can be influenced, for good or for bad, and why. The paper should not be more than 5 pages, double spaced.
3. Video recommendation *(10%)* : Find a video such a TED talk, movie, TV series relevant to what we discuss in this class. Write a one-page introduction and explain how it is relevant to the theme to recommend this piece to the rest of the class.
4. *Movie Reviews (10% each; 20% in total)* We will have movie days. As we are not meeting on campus, you will need to figure out a way to watch the movies on your own. You are expected to select two movies and write a review for each. A movie review shall be about 600-1000 words, providing a review of the stories (plot) and a critical analysis of how it is relevant to any themes covered in the class.
   You may also review one of the assigned movies while picking another movie (or a TV series, an episode of a TV series) to review on your own. In this case, check with the instructor if the movie you pick is relevant. The following titles will fit: *Minority Report*, *Person of Interest* (TV series) or some episodes of *Black Mirror*.
5. *Final Think Piece (20%):* This is your final. Based on course materials and your own experiences, what do you think is the biggest cybersecurity concern we face today? Explain why you think so and what you think we can do about it. It should be about 5 pages (double spaced) or slightly longer.

Deadlines

Living Connected Reflection (Due May 22)
First Movie Review (Due May 27)
Reading Responses (Due 3 Days from your selected date)
Second Movie Review (Due June 2)
Video Recommendation (Due June 5)
Final Think Piece (Due June 6)

Discussion Board and other forms of Participation (30%)
I will post discussion questions for each module. Out of the 15 discussion questions, you are expected to respond to at least 8 of them. You are also encouraged to initiate discussion and react to other students. Your grade will depend on the frequency, quality, and effectiveness of your participation. For example, it will be helpful if you bear mind that whenever you comment, try to include relevant, new information; also remember to convey your main points in the subject lines. In addition, you are encouraged to participate in other forms that may enhance your course experiences. For instance, your performance in the *Virtual Class Meeting or Office Hour* will be taken into consideration regarding your participation performance.

Manner of Online Interaction (netiquette):

1. Constructive criticism only. You know the difference. Help your classmates develop their thoughts, don't shut them out.
2. Be polite. We can't see your face or hear the tone of your voice, and you can't write an addendum to an offensive message you accidentally sent and have that addendum arrive first. Be careful and polite.
3. Don't take it personally but do take it professionally. Read what others are saying about what you posted not about who you are. Post back about what they posted not about who they are.
4. Build on your classmates' posts. Posting "I agree!" or "me, too" is usually uninformative for others. Posting the insights or new thoughts you had while reading someone else's post is much better.

Grade Dispute:
If you have any questions about your exam grade, you shall report to the instructor **within one week** from the time you receive the grade. You need to present a written appeal explaining why you think your grade should be changed. Please also bear in mind that disputing grade may end up with higher, lower or no change in your grade.

Academic Honesty:
As a University of Georgia student, you have agreed 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: www.uga.edu/honesty. Lack of knowledge of the academic honesty policy is not a reasonable explanation for a violation. Questions related to course assignments and the academic honesty policy should be directed to the instructor.

Topics and Modules

Day 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.

Day 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
* Chris Benner et al, "Still Walking the Lifelong Tightrope: Technology, Insecurity and The Future of Work," *Everett Program* (October 2018).

Day 3: Sources of Cyber Threats

* Tarah Wheeler, "Why the World Desperately Needs Digital Geneva Conventions," *Foreign Policy* (Fall 2018): 36-41.
* Symantec, "Internet Security Threat Report 2019," *Symantec Corporation*, pp. 14-58.
* CSIS, "Significant Cyber Incidents Since 2006," pp. 1-35.
* 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).

Day 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).

Suggested:

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

Day 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."

* The National Cybersecurity and Communications Integration Center, "Security Tip (ST06-005): Dealing with Cyberbullies," (August 31, 2018).

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

Day 6: Movie Day:

TERMS AND CONDITIONS MAY APPLY (2013)

-

Day 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," pp. 1-35.

Suggested:

** Brad Smith, "34 Companies Stand Up for Cybersecurity with a Tech Accord," Microsoft Blog (April 17, 2018).*

* Edwin Black, *IBM and the Holocaust* (Crown Publishers, 2001), Introduction.

* More technical details regarding the Target hack, see Xiaokui Shu et al, "Breaking the Target: An Analysis of Target Data Breach and Lessons Learned."

*Movie: **THE DEFENDERS (2018)**

Day 8: 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* (M

* 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).

Day 9: 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* (including something assigned previously):**
* CSIS, "Significant Cyber Incidents Since 2006," pp. 1-35.
* Kenneth Geers, Darien Kindlund, Ned Moran and Rob Rachwald, "World War C: Understanding Today's Advanced Cyber Attacks," Fireeye.

Day 10: 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.

Day 11: Movie Day

Enemy of the State (1998)

Day 12: Digital Authoritarianism (China as an Example)

* Rongbin Han, "Cyberactivism in China: Empowerment, Control, and Beyond," In *The Routledge Companion to Social Media and Politics*, eds. Axel Bruns et al. (Routledge, 2015): 268–80.
* 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.
* 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).
* Nicole Kobie, "The Complicated Truth about China's Social Credit System," *Wired UK* (January 21, 2019).
* Amy Hawkins, "The Odd Reality of Life under China's Orwellian Propaganda App," *Wired* UK (April 16, 2019).

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).

Day 13: Digital Challenges toward Democracy

* Kofi Annan, "How IT Threatens Democracy," *Project Syndicate* (Feb. 16, 2018).
* Alina Polyakova and Spencer P. Boyer, "The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition," *The Brookings Institution* (March 2018), pp. 1-18.
* 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).

* 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).

Suggested:
# Helmus et al, Russian Social Media Influence (Rand Corporation, 2018).

Day 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).
* Paul Mozur, “Google’s AlphaGo Defeats Chinese Go Master in Win for A.I.,” *The New York Times* (March 26, 2019).
* 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).

Day 15: Movie Day/Reflection Day

The Matrix (1999) or **Ex Machina (2014)**
* Also recommended:
The Matrix Reloaded
The Matrix Revolutions
Person of Interest