Coronavirus Information for Students

Face Coverings:

Effective July 15, 2020, the University of Georgia—along with all University System of Georgia (USG) institutions—requires all faculty, staff, students and visitors to wear an appropriate face covering while inside campus facilities/buildings where six feet social distancing may not always be possible. Face covering use is in addition to and is not a substitute for social distancing. Anyone not using a face covering when required will be asked to wear one or must leave the area. Reasonable accommodations may be made for those who are unable to wear a face covering for documented health reasons. Students seeking an accommodation related to face coverings should contact Disability Services at https://drc.uga.edu/.

DawgCheck:

Please perform a quick symptom check each weekday on DawgCheck—on the UGA app or website—whether you feel sick or not. It will help health providers monitor the health situation on campus: https://dawgcheck.uga.edu/

What do I do if I have symptoms?

Students showing symptoms should self-isolate and schedule an appointment with the University Health Center by calling 706-542-1162 (Monday-Friday, 8 a.m.-5 p.m.). Please DO NOT walk-in. For emergencies and after-hours care, see https://www.uhs.uga.edu/info/emergencies.

What do I do if I am notified that I have been exposed?

Students who learn they have been directly exposed to COVID-19 but are not showing symptoms should self-quarantine for 14 days consistent with Department of Public Health (DPH) and Centers for Disease Control and Prevention (CDC) guidelines. Please correspond with your instructor via email, with a cc: to Student Care & Outreach at sco@uga.edu, to coordinate continuing your coursework while self-quarantined. If you develop symptoms, you should contact the University Health Center to make an appointment to be tested. You should continue to monitor your symptoms daily on DawgCheck.

How do I get a test?

Students who are demonstrating symptoms of COVID-19 should call the University Health Center. UHC is offering testing by appointment for students; appointments may be booked by calling 706-542-1162.

UGA will also be recruiting asymptomatic students to participate in surveillance tests. Students living in residence halls, Greek housing and off-campus apartment complexes are encouraged to participate.

What do I do if I test positive?

Any student with a positive COVID-19 test is **required** to report the test in DawgCheck and should self-isolate immediately. Students should not attend classes in-person until the isolation period is completed. Once you report the positive test through DawgCheck, UGA Student Care and Outreach will follow up with you.

Mental Health and Wellness Resources:

- *If you or someone you know needs assistance, you are encouraged to contact Student Care and Outreach in the Division of Student Affairs at 706-542-7774 or visit https://sco.uga.edu. They will help you navigate any difficult circumstances you may be facing by connecting you with the appropriate resources or services.*
- *UGA has several resources for a student seeking mental health services (https://www.uhs.uga.edu/bewelluga/bewelluga) or crisis support (https://www.uhs.uga.edu/info/emergencies).*
- *If you need help managing stress anxiety, relationships, etc., please visit BeWellUGA (https://www.uhs.uga.edu/bewelluga/bewelluga) for a list of FREE workshops, classes, mentoring, and health coaching led by licensed clinicians and health educators in the University Health Center.*
- *Additional resources can be accessed through the UGA App.*

INTL 4666E Politics of Cyber Security

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

***** Subject to Updates *****
***** Please email the instructor or use the Debug link to report broken links or other problems you encounter *****

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.

Office Hour & Discussion Session
I will be hosting virtual office hour and discussion sessions weekly. Here is how to join the meetings:

Office Hours (Tuesday 12:15-13:00 EST; Contact the instructor should you need to meet at a different time)
https://zoom.us/j/98899846111

******

Zoom Discussion Session (11:30-12:30 Thursdays)

https://zoom.us/j/94179652069

******

Clarification: Attendance of the Zoom discussion meetings is one of the indicators of your participation. Should you have difficulty attending them, you need to more actively engage in other forms of participation to make it up.

Prohibition on Recording Lectures. In the absence of written authorization from the UGA Disability Resource Center, students may not make a visual or audio recording of any aspect of this course. Students who have a recording accommodation agree in writing that they:

- Will use the records only for personal academic use during the specific course.
- Understand that faculty members have copyright interest in their class lectures and that they agree not to infringe on this right in any way .
- Understand that the faculty member and students in the class have privacy rights and agree not to violate those rights by using recordings for any reason other than their own personal study.
- Will not release, digitally upload, broadcast, transcribe, or otherwise share all or any part of the recordings. They also agree that they will not profit financially and will not allow others to benefit personally or financially from lecture recordings or other course materials.
- Will erase/delete all recordings at the end of the semester.
- Understand that violation of these terms may subject them to discipline under the Student Code of Conduct or subject them to liability under copyright laws.

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	

Assignments & Deadlines (links to the Assignment Dropbox or the Discussions)

1. *Reading Responses (Due by Saturday of the week you pick) (15%)*: Write one response paper (about 5 pages, double spaced) based on the assigned readings for the week you choose (movie days excluded). The response may take a variety of forms, but should include a summary of basic ideas and arguments of ALL the readings, and more importantly your own questions, comments, and critical reflections. Feel free to draw on materials outside assigned readings. Please sign up for this assignment by picking the week. Please keep a record for yourself so that you don't miss the deadline.
2. *Video Recommendations (Due March 6)(10%)* : Find a video such a TED talk, movie, TV series relevant to what we discuss in this class that is not already included in the syllabus or course modules. Write a brief introduction to the material (by who, on what, how to access, etc) and then explain how it is relevant to the themes we discuss in this class as well as why you want to recommend it to the rest of the class. **Please post your recommendation on the discussion forum AND comment on each other's recommendation.**
3. *Midterm Reflection (Due March 24) (15%)* Document your Internet life as specifically as you can and then describe the (potential) scenarios in which you cut yourself off the Internet entirely for 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. There is no length limit. I expect it to be about 6 pages (or more), double spaced if you are being as specific as you can. Indeed, be specific and concrete rather than only stating your opinions in a general way.
4. *Movie Review (Due April 30) (5%)* We will have movie weeks. You are expected to select one movie and write a review. The 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. As we are not meeting on campus, you will need to figure out a way to watch the movies on your own.
   You may also pick 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 (Due May 5) (25 %):* This is your final. It should be about 10 pages (double spaced). You have to focus on the following topic when writing the think piece: Based on course materials and your own experiences, what do you think is **the single most grave cybersecurity concern** we face today (so do not make a very general statement and say everything is a cybersecurity conern or there are multiple cybersecurity concerns)? Explain why you think so and what you think we can do about it. Try to critically engage course materials while making a balanced argument.
6. Final quiz (10%). Quiz time to be annoucned. **Please make sure that you've gone through all course modules before taking the quiz. The quiz requires Respondus LockDown Browser, which may take a few minutes to install. For instructions, click here. If you are registered with DRC and needs extended time, please get in touch with the instructor as soon as you can.**
7. *Participation (20%)* For participation, there are three items. First, you are expected do ALL the readings and the course modules. Second, please engage in discussion via ELC for each module (you can directly respond to the discussion questions and/or react to other students; you can also inititate new discussion threads; your grade will depend on the frequency, quality, and effectiveness of your participation; **responding to at least 12 of all the discussion questions with decent quality to receive a grade of B or higher for this item alone.** And third, please attend the virtual office hours and or discussion sessions to interact with the instructor and other students. Note that if you are unable to attend the office hours or discussion sessions, you shall try to make it up by more actively participating in other forms that may enhance your learning experiences.
8. Due to the nature of the course (the large amount of writing assignments that are handed in either gradually or approaching the end of the semester), not all feedback to your assignments will be publicized on ELC (I will try). Please contact the instructor if you need more detailed feedback.

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.

No Further Distribution of Course Material
All video and audio recordings of lecturers and class meetings, provided by the instructors, are for educational use by students in this class only. They are available only through eLC for this course and are not to be copied, shared, or distributed. Recordings may not be reproduced, shared with those not enrolled in the class, or uploaded to other online environments. If the instructor plans any other uses for the recordings beyond this class, students identifiable in the recordings will be notified to request consent prior to such use. Classroom technology will be set up to record the instructor as well as the whiteboard and slides, but unless otherwise noted will only capture student voices, not student faces. Video and audio recordings by students are not permitted during the class unless the student has received prior permission from the instructor. Any sharing, distribution, and/or uploading of these recordings outside of the parameters of the class is prohibited. This also applies to the recording of Zoom meetings.

Topics and Modules

Week 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.

Week 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).

Week 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," 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).
* Adam Bannister, "Microsoft falls prey to SolarWinds supply chain cyber-attacks," The Daily Swig (December 18, 2020).

Week 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.*

Week 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

Week 6: Movie Week

TERMS AND CONDITIONS MAY APPLY (2013)

Week 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."
ALSO SUGGESTED: THE DEFENDERS (2018). NOTE THIS IS NOT THE MARVEL'S MOVIE.

Week 8: Movie Week

*Documentaries/Movies: **THE SOCIAL DILEMMA (2020)**

Week 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).

Week 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 **(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.

Week 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.

Week 12: Movie Day

Enemy of the State (1998)

Week 13: 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).
* 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).

Week 14: 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).
* 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," T*he 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).

Week 15: 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).

Week 16: Movie Day/Reflection Day

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