HDCC 106: Internet of Evil

Dr. Daniel Greene
College of Information Studies
Hornbake South, Room 4105D

dgreene1@umd.edu

Schedule office hours via
https://calbird.com/daniel-greene/students

Trevor Paglen's *Vampire (Corpus: Monsters of Capitalism)*,
"Adversarially Evolved Hallucination" (2017).

"Don't be evil. We believe strongly that in the long term, we will be better served--as shareholders and in all other ways--by a company that does good things for the world even if we forgo some short term gains. This is an important aspect of our culture and is broadly shared within the company."

- Google Inc. investor prospectus (2004)

"We believe that Google should not be in the business of war....We cannot outsource the moral responsibility of our technologies to third parties."

- Employee letter to Google CEO Sundar Pichai (2018)

CATALOG DESCRIPTION
Examining the antagonists trying to exploit, break, trick, and brick modern information systems: trolls, spammers, viruses, hackers, dictators, and more. Exploring the technical and historical background of internet evildoers, how the meaning of 'evil' varies between systems and cultures, and how complex networks and the techniques to support them co-evolve with their evil adversaries. Students develop practical and theoretical skills in threat assessment, design methods, and social research.

COURSE DESCRIPTION
Over the last few years, the shine of Web 2.0 has worn off. Where Facebook, for example, was

once celebrated as a global community built by entrepreneurial idealists, it is now feared as a fake news engine and a coordination mechanism for extrajudicial violence, overseen by heartless libertarians. We've learned that new connections implied new vulnerabilities, individual and systemic. This course gives students the practical and conceptual tools to navigate this shifting terrain. It is a design course, where we will take an adversarial approach to the core infrastructure of the information economy--learning to both break it and save it. It is also a philosophy course, where we will ask what 'evil' means and whether and how institutions or technologies can be 'evil.' And it is a science, technology, and society course, where we explore how the meaning of 'evil' evolves within and between different communities and the technologies on which they run.

Throughout the semester, students will read and practice skills from each of these fields--and more--as they develop a 'security mindset'. We will explore the relationship between evil and information technology at successively larger scales, beginning with evil designs (e.g., spamming systems), moving on to evil organizing (e.g., coordinated harassment campaigns), and ending with a focus on evil institutions (e.g., state use of digital tools for ethnic cleansing). Students will study and respond to internet evil by researching an historical scam and demoing their own technologically-delivered scam. Intermittent quizzes will ensure students stay on top of our readings, while informal current events presentations will extend our class discussions beyond what's on the syllabus.

STUDENT LEARNING OUTCOMES

At the conclusion of this class, you should be able to:

- Demonstrate a 'security mindset' in your approach to different sociotechnical problems
- Demonstrate critical thinking in evaluating the relationship between human values, organizational structures, and technological designs.
- Take an adversarial approach to design: On the one hand, identifying existing technical and social vulnerabilities and creating new ones, on the other hand, explaining to others how to secure those vulnerabilities.
- Explain how and why the nature of 'evil' changes based on the community and the infrastructure involved, and who benefits or suffers from the designation.
- Conduct archival research that identifies historical primary sources relevant to contemporary debates.

ASSIGNMENTS

Each assignment will have a detailed rubric and instruction sheet to accompany it. Larger assignments require an outline and a meeting with the instructor ahead of their delivery date, we will also hold informal brainstorming discussions in class. Larger projects can be completed in a pair, but the deliverables will be somewhat longer--tell the instructor before the outline stage if you're thinking of this. Assignments add up to 1000 points.

Historical Evil: 200 points (25 points for a topic suggestion, 75 points for an outline and instructor meeting, 100 points for research paper)

Students will pick an historical example of an evil design, broadly construed, and write a 750-word research brief describing its designers, goals, targets, methods, and outcomes. 'Evil design' here is broadly construed to include everything from confidence schemes to ransomware, pre-Web spam election fraud. The report could review a type of scam, like the Spanish Prisoner, or a specific incident like the Creeper virus. Students will need to use contemporary sources (e.g., historical newspapers, trade literature) to provide evidence. The evildoing must take place prior to 1995 (an arbitrary birth-year for the Web). Students may complete this in pairs, but this will require a 1000-word report.

Original Evil: 250 points (25 points for a topic suggestion, 75 points for an outline and instructor meeting, 100 points for research paper, 50 points for final presentation)

Students will design and demonstrate a new scam, broadly construed, with clearly identified goals, targets, methods, and desired outcomes. 'Scam' here is broadly construed to include everything from confidence schemes to ransomware. Students will write a short essay (~500 words) explaining their scam and will demonstrate it by whatever means they choose: A deepfake video, specific phishing emails, the map of a planned burglary of finals' Scantrons etc. For their final presentation, students will 'get the team together' a la *Ocean's 11* and explain to the class what they need to do to pull off the scam, why it will work, and how the target might stop them (e.g., technical, social, or policy defenses). Students may complete this in pairs, but this will require a 750-word report and a slightly longer presentation. Students will not, under any circumstances, release their scam into the world and do crimes.

Reading Quizzes: 150 points

There will be 11 pop quizzes assigned on ELMS. You will have 48 hours in which to complete them but only 15 minutes to finish the quiz once you start it. The lowest-scoring quiz will be dropped at semester's end. Quizzes are designed to be easy: If you've done the reading up to the point at which the quiz opens, you'll ace the quiz.

Current Events Presentation: 100 points

Students will be assigned a day of class for which they will prepare a 500-word essay relating the day's reading(s) to a story from the news (if we're reading more than one thing, feel free to focus on just one). Students will also prepare an informal 5-minute presentation summarizing their essay, along with discussion questions meant to guide the day's session.

Participation: 250 points

Students are not graded on attendance but on their active participation in class. Every class will include some sort of written warm-up exercise that sets the stage for later discussions activities. Participating in both is essential to receive full credit for that day. *Four 'freebie' days are built into this grading scheme, so students should not feel obligated to request an excused absence for any given day just to recover that day's participation points.*

Capstone Ideas Workshop [DCC Program Requirement]: 50 points (all-or-nothing)

You must attend one "Capstone Ideas" workshop this semester, organized by DCC staff. Dates for these workshops are on the DCC events calendar on the website, where you will sign up for this workshop. This workshop is designed to help you think through possible projects you can pursue next year in for your Capstone project. You are also required to attend some portion of the DCC Capstone Fair (held in the MPR on the last day of class: Tuesday, May 12 from 6-8pm). Students who are enrolled in courses that conflict with the entire duration of the Capstone Fair can be given accommodation for this part of the grade with prior approval of the professor. You must also log 5 Studio Hours in the Lab or Sound Studio by self reporting with a Lab manager. Students receive 50 points for completing all requirements.

CLASS SCHEDULE

Unit 1: Evil Foundations

Week 1: Introductions

Monday January 27
Readings:
- None!

Wednesday January 29
Readings:
- Listen to the "Snapchat Thief" episode of the *Reply All* podcast. It's about an hour.
- Schneier (2008). "The security mindset." *Schneier on Security*.

Week 2: Adversarial design

Monday February 3
Readings:
- Agre (2003). "Your Face Is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places"
- Meyer (2016). "Anti-surveillance camouflage for your face"

- [Harvey (2013). "Face to Anti-Face"](#)

<div align="center">Wednesday February 5</div>

Readings:
- [Jeong (2018). *Internet of Garbage*](#). The Verge.

Unit 2: Evil Designs

Week 3: Original Sins Part 1

<div align="center">Monday February 10</div>

Readings:
- Manaugh (2016). "Space invaders" in *A Burglar's Guide to the City.* [ELMS]

<div align="center">Wednesday February 12 [class held in McKeldin]</div>

Readings:
- Excerpt from Maurer (2010) *The Big Con: The Story of the Confidence Man* [ELMS]

Week 4: Original Sins Part 2

<div align="center">Monday February 17</div>

Readings:
- Rose (2004) "The Body of Evil" [ELMS]

<div align="center">Wednesday February 19</div>

Readings:
- Excerpt from Brunton (2013) *Spam: The Shadow History of the Internet* [ELMS]

Topic Briefs for Historical Evil Project due by midnight Thursday February 20

Week 5: Haunting and Hacking

<div align="center">Monday February 24</div>

Readings:
- Excerpt from Schneier (2018). *Click here to kill everybody: Security and survival in a hyper-connected world* [ELMS]
- [Maughan (2015). "Be good for goodness' sake."](#)

<div align="center">Wednesday February 26</div>

Readings:
- McKinney & Mulvin (2019) "Bugs: Rethinking the History of Computing"

Week 6: Harassment

<div align="center">Monday March 2</div>

Readings:
- Freed et al (2018). "'A stalker's paradise': How intimate partner abusers exploit technology."
- Pluspluspodcast (2017) "Domestic surveillance" [available on all podcast platforms]

<div align="center">Wednesday March 4</div>

Readings:
- Douglas (2016). "Doxing: A conceptual analysis." *Ethics and Information Technology*

Historical Scam Outlines due by midnight Thursday March 5

Unit 2: Evil Organizing

Week 7: Hate

<div align="center">Monday March 9</div>

Readings:
- Excerpt from Daniels (2009). *Cyber Racism: White Supremacy Online and the New Attack on Civil Rights.* [ELMS]
- Partin (2020). "What if modern conspiracy theorists are altogether too media literate?"

<div align="center">Wednesday March 11</div>

Readings:
- Smith (2017). "In the early 1980s, white supremacist groups were early adopters (and masters) of the internet"
- Tufeck (2018). "YouTube: The Great Radicalizer."
- Lewis (2020). "All YouTube, Not Just the Algorithm, is a Far-Right Propaganda Machine"

Spring Break

Monday March 23

Readings:
- Dibbel (1998) "A rape in cyberspace (or, a Tiny Society and How to Make One)"
- "When is a troll no longer a troll?" [Video]

Wednesday March 25

Readings:
- Philips (2018). "The oxygen of amplification: Better practices for reporting on extremists, antagonists, and manipulators."
- Play Troll Factory https://trollfactory.yle.fi/

Historical Evil Projects due by midnight Thursday March 26

Week 9: Moderation

Monday March 30

Readings:
- Excerpt from Gillespie (2018). *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* [ELMS]
- Chen (2015). "The laborers who keep dick pics and beheadings out of your facebook feed."

Wednesday April 1

Readings:
- Hopkins (2017). "Revealed: Facebook's internal rulebook on sex, terrorism and violence." *The Guardian.*
- Facebook *Terms of Service*
- Facebook *Community Standards*

Original Evil Topic Briefs Due Midnight April 2

Week 10: Surveillance

Monday April 6

Readings:
- Trujillo & Vitale (2019). "Gang takedowns in the De Blasio era: The Dangers of Precision Policing."

- [Smith (2018). "Former Baltimore Police Officer Unloads On The Department's Gang Database."](#)

Wednesday April 8

Readings:
- Browne (2012). "Everybody's got a little light under the sun: Black luminosity and the visual culture of surveillance."

Unit 3: Evil Institutions

Week 11: Infrastructure

Monday April 13

Readings:
- Excerpt from Arendt (2006 [1964]) *Eichmann in Jerusalem: A report on the banality of evil* [ELMS]

Wednesday April 15

Readings:
- [Black (2001). "The Nazi Party: IBM and 'Death's Calculator'"](#)

Original Evil Outlines due by midnight Thursday April 16

Week 12: Responsibility

Monday April 20

Readings:
- Mod (2016). "[The Facebook-loving farmers of Myanmar."](#)
- Fink (2018). "Dangerous speech, anti-Muslim violence, and Facebook in Myanmar." [ELMS]

Wednesday April 22

Readings:
- Burrington (2017). "[Could Facebook be tried for human rights abuses?"](#)
- [Steceklow (2018). "Why Facebook is losing the war on hate speech in Myanmar?"](#)

Week 13: Fake News

Monday April 27

Readings:

- Marwick (2017). "Why do people share fake news? A sociotechnical model of media effects."

Wednesday April 29

Readings:
- Karpf (2019). "On digital disinformation and democratic myths."
- Turner (2018). "Machine politics: The rise of the internet and new age of authoritarianism."

Original Evil Projects due by midnight Thursday April 30

Week 14: Don't Be Evil

Monday May 4

Readings
- Irani (2018). "A cloud is not just a cloud."
- Tarnoff and "Kim" (2018). "Tech workers against the Pentagon."

Wednesday May 6

Presentations

Week 15: Presentations

Monday May 11

Presentations