Cognitive Security: Defence against Disinformation

INST 408C
Fall 2021

Course Description

Cognitive security is the application of information security principles, practices, and tools to misinformation, disinformation, and influence operations. It takes a socio-technical lens to high-volume, high-velocity, and high-variety forms of "something is wrong on the internet".

This course starts with the ways that users and groups are influenced online, from user experience, marketing, adtech and online political campaigns through to astroturfing, online psyops, disinformation campaigns. We'll look at the techniques and tactics used to create influence, the tools, methods and design patterns being created to detect, counter and mitigate against it, the emerging discipline of cognitive security and how it meshes with other work including information security, machine learning and geopolitics.

The course is practical, arranged around a set of python notebooks and open-source tools, but also rooted in deep theories of why and how disinformation campaigns happen.

Learning Outcomes

After successfully completing the course, students will be able to

- Elaborate how information security and cognitive security interact
- Evaluate persuasive technology at different scales
- Evaluate influence operation mechanisms and tracking techniques
- Use tools to investigate account and network-level coordinated inauthentic activities
- Understand ethical behaviour around misinformation and disinformation response and research

Required Resources

All course materials will be available on our course website: **elms.umd.edu**

SJ Terp
sjterp@umd.edu
she/her
Means "hill" in Dutch

Class meets
Monday/Wednesday
2:00 PM - 2:50 PM
WDS 1114

Office hours
Monday/Wednesday
3:00 PM - 4:00 PM
PTX 2114

Prerequisite:
None

Course communication
I will announce any changes to the syllabus or other important information on ELMS. You may choose to have such announcements sent to you in your preferred manner through the ELMS interface.

To contact me, please send me an email at the address above and I will get back to you within 24 hours. If the communication is less urgent, feel free to message me on ELMS.

Expectations and Grading Procedures

Composition of percentage grades

In class activities: 50%

Case studies: 30%

- ***3 case studies, 10% per study***

Problem challenge (20%)

- In this project, you will identify a problem, use the lens of one of the frameworks we studied in class to address it, and explore/analyze *theoretically* how to successfully measure and counter it.

Converting percentage grades to letter grades

I follow the standard practice in converting percentage grades to letter grades, as listed in the table below.

Letter	Points	Lower bound
A+	4.0	97
A	4.0	94
A-	3.7	90
B+	3.3	87
B	3.0	84
B-	2.7	80
C+	2.3	77
C	2.0	74
C-	1.7	70
D+	1.3	67
D	1.0	64
D-	0.7	60
F	0.0	0

Campus Procedures and Policies

It is our shared responsibility to know and abide by the University of Maryland's policies that relate to all courses, which include topics like:

- Academic integrity
- Student and instructor conduct
- Accessibility and accommodations
- Attendance and excused absences
- Grades and appeals
- Copyright and intellectual property

Please visit www.ugst.umd.edu/courserelatedpolicies.html for the Office of Undergraduate Studies' full list of campus-wide policies and follow up with me if you have questions.

Policy on Academic Misconduct. Cases of academic misconduct will be referred to the Office of Student Conduct irrespective of scope and circumstances, as required by university rules and regulations. It is crucial to understand that the instructors do not have a choice of following other courses of actions in handling these cases. There are severe consequences of academic misconduct, some of which are permanent and reflected on the student's transcript. For details about procedures governing such referrals and possible consequences for the student please visit http://osc.umd.edu/OSC/Default.aspx

It is very important that you complete your own assignments, and do not share any files or other work. The best course of action to take when a student is having problems with an assignment question is to contact the instructor. The instructor will be happy to work with students while they work on the assignments.

University of Maryland Code of Academic Integrity. The University of Maryland, College Park has a nationally recognized Code of Academic Integrity, administered by the Student Honor Council. This Code sets standards for academic integrity at Maryland for all undergraduate and graduate students. As a student you are responsible for upholding these standards for this course. It is very important for you to be aware of the consequences of cheating, fabrication, facilitation, and plagiarism. For more information on the Code of Academic Integrity or the Student Honor Council, please visit http://shc.umd.edu/SHC/Default.aspx

Note on Turnitin Originality Checker and Plagiarism. For this course, some of your assignments may be collected via Turnitin on our course ELMS page. I have chosen to use this tool because it can help you improve your scholarly writing and help me verify the integrity of student work. For information about Turnitin, how it works, and the feedback reports you may have access to, visit Turnitin Originality Checker for Students.

Even for assignments that do not require you to submit through Turnitin, you are responsible for confirming that anything you submit does not contain plagiarism. This includes not including proper formatting to indicate when you directly quote or paraphrase another source. If you do not know how to correctly cite material, refer to the UMD Library resources, available at https://lib.guides.umd.edu/c.php?g=327184&p=2588295.

If you are found to have committed plagiarism, you will receive a zero on that assignment. You can resubmit the assignment within one week with a 50% penalty. If you violate Academic Integrity more than once, you will receive a zero in the class and will be referred to the Student Honor Council.

Special Needs. Students with disabilities should inform the instructor of their needs at the beginning of the semester. Please also contact the Disability Support Services (301-314-7682 or http://www.counseling.umd.edu/DSS/). DSS will make arrangements with the student and the instructor to determine and implement appropriate academic accommodations. Students encountering psychological problems that hamper their course work are referred to the Counseling Center (301-314-7651 or http://www.counseling.umd.edu/) for expert help.

Course Schedule

Note: readings may be added/changed throughout the semester. I will notify you by email if this is the case.

Week	Date	In class	Class preparation	Deliverables
1	8/30	**Lecture: course overview, introduction** Outline: • Introduces students to the contents of the course, and supporting materials needed to work on disinformation data. • History of cognitive security • Working definitions of information operations, disinformation, and cognitive security • Disinformation examples and common myths • Where to find more information		**in-class exercise: definitions and examples of mis/disinformation, rumours, conspiracies, information operations**
1	9/1	Lecture: disinformation reports, ethics • Example disinformation analyses. • Students will comment on existing disinformation analyses, and start their own research outlines. • How to investigate safely • Ethics of handling data from and about people, and groups already working on disinformation. • Outcome: students will be able to articulate needs and pitfalls of disinformation research, and will have started their own research outlines. Lecture: researcher risks • Potential risks to influence operations investigators, and mitigations for them. • Operational security	**Read:**	Exercise: List and examine the risks in an existing influence operation. **in-class** exercise: comment on existing disinformation analyses

		• Mental health • Ethics and the golden rule ("first, do no harm") • Outcome: mitigation strategies for personal risks inherent in investigating them.		
2	**9/6**	NO CLASS: Labor day		
2	**9/8**			
3	**9/13**	**Lecture: cognitive security fundamentals** Outline: • Assessing social media misuse - channels, influencers, groups and messaging • An introduction to actors, behaviours, techniques, tools • The disinformation pyramid. Example incidents, example narratives. • Information operations as an information system Details: • Introduces students to disinformation, misinformation, propaganda, information operations; their creators, outputs, mechanics and effects. Also introduces students to live feeds of disinformation-containing data. • Outcome: students will be able to articulate disinformation campaign mechanics and motivations.		In-class exercise: use Hypothes.is to track misinformation materials Assignment: Track a misinformation or disinformation narrative across the internet and/ or traditional media.
3	9/15	**Cognitive security risks** • Risks created by misinformation and influence operations • Frameworks for assessing cognitive security risks • Outcome: a framework for assessing influence operation risks		

4	**9/20**	**Human system vulnerabilities and patches** Outline: ● From clicks to disinformation ● cognitive biases and their abuses ● the range of ways users and groups are influenced online (and offline via online means) - user experience, marketing and adtech, online political campaigns, astroturfing, online psyops, disinformation campaigns.		
4	**9/22**	Psychology of influence ● Outcome: articulate common influence techniques. ● Applying marketing models ● The medium is the message: Content vs Context		Exercise: List and categorise online and offline advertising seen in an hour
5	**9/27**	**Frameworks for understanding cognitive security** Outline: ● Layer-based models ● Object-based models ● Behaviour-based models ● Introduces students to infosec-related models of information operations and disinformation, with examples of their use and connection to other information security practices. ● Outcome: students will be able to evaluate disinformation incidents and their components		
5	**9/29**	Relational frameworks ● Group-based models ● (Network-flow models)		Exercise: apply frameworks to existing disinformation analyses.
6	10/4	**Building Landscapes** Outline: ● Building an information landscape ● Building a risk landscape ● Building a response landscape ● Landscape interactions ● Landscape patches Details: ● Introduces landscapes: assessments of the cognitive security situation in a region, country, vertical, or business. Gives examples of desk surveys,		

		country-level investigations, and information interviews to improve models and knowledge of an area. Introduces cognitive security gap analysis. • Outcome: students will be able to assess disinformation risk in a country, business, or vertical Case study assignment: • build a disinformation landscape assessment for a country, business, or vertical		
6	**10/6**			Exercise: build landscapes from existing disinformation assessments (e.g. the Oxford Internet Institute's annual country summaries)
7	**10/11**	**Setting up an investigation** Outline: • Setting up a process • Choosing tools • Collecting data (social, text, image) • Building investigation communities • Overlapping communities: cognitive security, OSINT, information security. • How to send data to responders Practical: • Introduces students to streaming data APIs, large datasets, and cleaning, exploration and storage methods for large data, including simpler automations • Outcome: students will be able to access and store larger datasets, and have basic analysis tools for them		
7	**10/13**		Read https://si.ma/fb-cib/	
8	**10/18**	**Misinformation data analysis** Outline: • Setting up your notebooks • Keeping track of what you've found Details:		

		• Introduces techniques and tools for assessing misinformation artifacts: images, text, accounts, groups, domains etc. • Exercise: analyse a dataset containing misinformation artifacts • Outcome: students will be able to track and assess misinformation artifacts		
8	**10/20**	• Artifact analysis • Text analysis		
9	**10/25**	Disinformation data analysis Outline: • Social network analysis: Mapping and measuring relationships and information flows between people, groups, URLs, and other information entities. Details: • Introduces techniques and tools for assessing the relationships between disinformation artifacts, narratives, and other incident objects. • Outcome: students can apply network tools to find and assess anomalies in social media artifact relationships.		
9	**10/27**			Exercise: apply network analysis tools to a dataset containing potential disinformation
10	**11/1**	**Disinformation responses** Outline: • Responder types • Building response communities • Message-based responses: countermessaging, prebunking, debunking • Action-based responses • First, do no harm Details: • Describes the types of misinformation and disinformation response groups that exist, and the types of responses that they can and do implement.		

		Shows how to share information between responding groups. ● Exercise: assess the capabilities of existing response groups ● Outcome: students can articulate response types available to different response groups, and potential effects from them. Case study assignment: gather datasets related to an existing disinformation narrative, and package them as an alert or report to be sent to a disinformation response group.		
10	**11/3**			
11	**11/8**	**Monitoring and Evaluation** Outline: ● Measuring cognitive security effects and responses ● Applied cynicism: statistics and models Details: ● Covers the measurement of disinformation risk, disinformation actions, and response actions, at tactical and organisational levels. ● Exercise: M&E assessment of an existing misinformation response (e.g. WHO response to Covid19 infodemic) ● Outcome: students will have tools to assess how effective disinformation events and their responses are.		
11	**11/10**			
12	**11/15**	**Games, red teaming and simulations** Outline: ● Games ● Disinformation red teams ● Simulations Details: ● Introduces the use of games and other simulations to help understand disinformation tactics and potential responses to them.		**Exercise: design a disinformation-based game**

		• Exercise: Test out a game, then red-team an existing disinformation incident. • Outcome: students can use tools and simulations to assess, plan, and change disinformation responses		
12	11/17	**Cognitive Security red teaming** • Exercise: red-team a disinformation as a service business and potential counters to it		
13	11/22	**Project work**		**Proposal for end of term project.**
13	11/24	**NO CLASS: Thanksgiving**		
14	11/29	**Project work session**		
14	12/1	**Cognitive Security as a Business** Outline: • Disinformation as a service models • Financial motivations and estimates • Business effects of disinformation Details: • Introduces business models behind disinformation and cognitive security. Goes into detail on the potential business attack vectors and effects from disinformation and hybrid campaigns that include disinformation (e.g. hacking, malware etc). • Outcome: students can articulate disinformation business models		
15	12/6	**Future Possibilities** Outline: • Cognitive security and business - potential directions • Health sector: medical misinformation trends in Covid19 and Vaccine hesitancy • Elections: trends around the world • Responses: trends around the world Details • Looks at potential future arcs for disinformation incidents and response.		**Project presentations**

		• Outcome: students can articulate potential futures in misinformation, disinformation, and responses to them.		
15	12/8	**Project Presentations** **Outline:** • **Students present their group projects** **Details:** • **Students give 10-minute presentations on their group projects.** • **Outcome: students have performed an end-to-end misinformation or disinformation incident analysis.**		
16	12/13	**Summary and connections**		
final	TBD			