PUBP-8803 Syllabus

Cyber Threat Intelligence – 3 Credits

Instructor Information

Instructor: Sergio Caltagirone

Email: [redacted]

General Course Information

Description

Cyber threat intelligence (CTI) and threat hunting identify and track novel threats to produce critical knowledge and insight that improves decision-making and reduces harm from cyber threats, online disinformation, and digitally mediated abuses of power that affect individuals, organizations, institutions, and societies including the civil liberties and critical infrastructure they rely upon.

This introductory course takes you into the intricate world of contemporary "spy versus spy" activity in cyberspace, where states, activists, organized crime, authoritarian regimes, and extremist groups use offensive cyber operations, espionage, and effects to harm and influence others. You will learn how to find, analyze, and communicate cyber threats and their risk to decision-makers while also learning to read and integrate the intelligence produced by others into coherent, evidence-based threat knowledge.

While we spend a lot of time on the technical aspects of cyber threats to find and expose their operation, we will also learn how to analyze the broader societal and cultural elements surrounding cyber operations. Intelligence analysts must be trustworthy and effective communicators of cyber threat knowledge and risk, and we will learn to manage our conscious and unconscious bias regarding cyber threats, actors, and victims to protect our integral role in the cybersecurity defense and policy communities. As such, we will not limit ourselves to "Fortune 500" cybersecurity when there are abundant resources to protect oneself. We will also learn how to find and analyze offensive cyber operations that have an unequal impact across different communities such as public services, local utilities, small businesses, journalists, civil society, and vulnerable populations.

Each student will receive a project topic and a customer (hypothetical or real). Customers may range from public agencies and private businesses to non-profit organizations and

communities that are at particular risk of being targeted by cyber operations. The student will execute the entire intelligence cycle and threat hunting methodology to satisfy the customer's information needs, paying attention not only to technical indicators but also to issues such as non-cyber impact and the broader social and policy context. The student will incorporate cyber defense and threat mitigation for decision makers such as technical defense, detections, and policy recommendations.

You will learn the fundamentals of cyber threat intelligence production: collecting, processing, analyzing, documenting, and disseminating new information about cyber threats in a manner that is rigorous, transparent, and accountable. We will briefly introduce theoretical lenses from critical security studies and illustrate how assumptions, institutional bias and power dynamics can shape both cyber threat activity and the ways analysts interpret it.

You will also develop the ability to collect, critique, consume, and use intelligence produced by others, evaluating sources for credibility, propaganda, funding bias, and other forms of manipulation that can undermine effective cyber defense.

Through a blend of conceptual discussion and practical exercises, students will unearth and analyze cyber threat activity using the same tools and methodologies as professionals in threat intelligence and threat hunting roles, while learning to communicate findings clearly to technical and non-technical stakeholders, including those working in cyber defense, policy, and governance.

This course will expect you to apply both technical cybersecurity skills and critical policy analysis equally.

Course Learning Outcomes

- Implement the stages of the intelligence cycle using cyber threat intelligence tradecraft
- Develop and test cyber threat hunting hypotheses to find new threats
- Use industry-standard tools, data sources, and tradecraft to collect, find, and analyze a significant cyber threat
- Produce intelligence that satisfies a requirement and meets the standards of professional intelligence analysis

Required Course Materials

All materials instructor-provided

Grading Policy:

Your final grade will be assigned as a letter grade according to the following scale:

A 90-100%

B 80-89%
C 70-79%
D 60-69%
F 0-59%

According to policy, grades at Georgia Tech are interpreted as follows:

A Excellent (4 quality points per credit hour)
B Good (3 quality points per credit hour)
C Satisfactory (2 quality points per credit hour)
D Passing (1 quality point per credit hour)
F Failure (0 quality points per credit hour)

See http://registrar.gatech.edu/info/grading-system for more information about the grading system at Georgia Tech.

Description of Graded Components

This course omits midterms and finals.

We will evaluate you using a project and quizzes.

PROJECT A four-part project following the intelligence cycle (each worth 20% of your final grade)

1. Research and Requirements
2. Tools, Data, and Collection Strategy
3. Analysis
4. Dissemination

QUIZZES Additionally, there will be three 60-minute timed quizzes covering lectures and assigned readings – total worth 20% of your grade.

Each week will require at least 5 hours of reading/watching material, researching, and writing outside of class.

External Expectations

This course requires the students to engage and interact with external cybersecurity professionals and executives. The students will act with utmost professionalism during all interactions. Furthermore, students are required to sign an ethics pledge protecting the identity of their external mentor as well as protect sensitive and proprietary information.

Communication

All official course communication will occur over Canvas – students are expected to monitor Canvas for all course updates.

Late Assignments

The instructor reduces assignments by 10% per day when students submit them after the deadline, except with institute-approved delays or absences, or prior instructor-approved delays.

Remote Meetings

The instructor works away from Atlanta over 50% of the time, and therefore there will be several remote classes held via Teams or Zoom. If the institute announces a digital learning day at the scheduled course time, we will conduct class remotely.

Course Policies

Attendance and/or Participation

The instructor does not take attendance in this class, although they expect you to know and apply the lecture material along with the material covered on the quizzes.

Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. Review Georgia Tech's Honor Code and the student Code of Conduct.

Any student suspected of cheating or plagiarism on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services (404-894-2563) as soon as possible to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Student-Faculty Expectations Agreement

At Georgia Tech, we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. The Student-Faculty Expectations articulate some basic expectations that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Artificial Intelligence

We expect and encourage you to use artificial intelligence tools in class to enhance your work. However, you should treat all tools like tools or the same as your peers. You would not copy what your peer writes and submit the work as yours; the same as you will not copy what any AI tool authors and submit the work as yours. That constitutes plagiarism, and we will treat it as such (see Academic Integrity). AI tools in this class are strictly for research and peer testing, never for authorship or your presentation slides, presentation speaking notes, nor your written reports. You are expected to submit 100% original material. IF you use an AI tool, you will treat it as if it were an outside reference and properly cite it using recognized academic citation practices.

Campus Resources for Students

Graduate Student Academic and Professional Success Resources:

A list of resources for graduate students is given on the Office of Graduate and Postdoctoral Education website. Specific information for current graduate students includes

- Academic Resources such as the Communications Center, Language Institute, Library, Catalog, Registrar, resources for conducting research, Advocacy and Conflict Resolution resources, and how to manage unexpected situations that may impact your academic performance;
- Student Resources such as Campus Services, Child Care/Family programs, Health & Wellness, Career Services, and the Student Resource Guide; and
- *Professional Development such as the programming from the Career Center and other professional development resources and events"*

Student Well-Being:

At Georgia Tech, we are concerned about your overall physical, social, and mental well-being. A comprehensive list of wellness related resources has been compiled and maintained by the Office of the Vice President for Student Engagement and Well-being (student-resource-guide (gatech.edu)