COURSE TITLE: CYBER THREAT INTELLIGENCE, DFOR 780-001

SEMESTER: Spring 2024

INSTRUCTOR & COURSE INFORMATION:

DAVID SIGEL
Office Hours: By appointment
Email: dsigel@gmu.edu

Class Meeting Location: TBD
Class Meeting Times: Wednesday, 07:20 – 10:00pm ET
Mode of Instruction: In-Person
Course Pre-Requisites: N/A

COURSE DESCRIPTION: This course provides a comprehensive overview of cyber threat intelligence, its methodologies, and its application within the context of a cyber fusion center/team and to the cybersecurity industry overall. Through the study of case studies and hands-on exercises, students will learn how to assess, analyze, and mitigate potential cyber threats.

COURSE GOALS:

- Develop an understanding of the principles of cyber threat intelligence.
- Develop the ability to analyze and interpret intelligence data to identify and assess cyber threats.
- Enhance the ability to develop effective strategies for mitigating cyber risks.
- Explore emerging technologies in cyber threat intelligence.

LEARNING OBJECTIVES:

- Explain the concept and principles of cyber threat intelligence.
- Describe the sources of intelligence data and methods for collecting it.
- Analyze and interpret intelligence data to identify and assess cyber threats.
- Develop effective strategies for mitigating cyber risks.
- Understand emerging technologies, such as machine learning and artificial intelligence, to enhance cyber threat intelligence.

COURSE POLICIES:

1. **Communication Policy:** All communication outside of classroom or not previously scheduled between Instructor and Student(s) will be conducted through official George Mason email and Blackboard.
2. **Assignment/Project Guidelines:**
   - All written assignments/projects should follow the following format:
     i. Calibri Body 10-pt font with 1-inch margins, single-spaced.
     ii. 1" margins (NOTE: Microsoft defaults to 1.25" margins, so you will need to adjust them).
     iii. Utilizes a minimum of 5 varied, 'reputable' sources, government reports, etc. If you are doubtful about whether a source is reputable, have your Team Leader discuss it with the Instructor.
     iv. Use of graphs and/or images is encouraged, especially when used to help readers understand your subject matter. Remember to cite them (usually right next to the map/image, rather than in the bibliography).
     v. APA Citation and references (cite images, too).
     vi. List of references
3. **Campus Closure or Emergency Class Cancelation/Adjustment Policy**
   - If the campus closes, or if a class meeting needs to be canceled or adjusted due to weather or other concern, students should check Blackboard [or other instruction as appropriate] for updates on how to continue learning and for information about any changes to events or assignments.
4. **Academic Integrity**
   - The integrity of the University community is affected by the individual choices made by each of us. As a Mason student, you should follow these fundamental principles at all times, as noted by the Honor Code: (1) All work submitted should be your own, without the use inappropriate assistance or resources, as defined by the assignment or faculty member; (2) When you use the work, the words, the images, or the ideas of others–including fellow students, online sites or tools, or your own prior creations–you must give full credit through accurate citations; (3) In creating your work, you should not take materials you are not authorized to use, or falsely represent ideas or processes regarding your work. If you are uncertain about the ground rules or ethical expectations regarding the integrity of your work on a particular assignment or exam, you should ask your instructor for clarification. Support for you to complete your work is available; no grade is important enough to justify academic misconduct.

i. ***Statement Regarding Use of Generative AI Tools***: Minimum statement: Any student use of Generative-AI tools should follow the fundamental principles of the Honor Code.

ii. ***Statement Regarding the Use of Study Sites***: Some kinds of participation in online study sites violate the Mason Honor code: these include accessing exam or quiz questions for this class; accessing exam, quiz, or assignment answers for this class; uploading of any of the instructor's materials or exams; and uploading any of your own answers or finished work. Always consult your syllabus and your professor before using these sites.

5. **Basic Course Technology Requirements**
   - Activities and assignments in this course will regularly use the Blackboard learning system, available at https://mymason.gmu.edu. Students are required to have regular, reliable access to a computer with an updated operating system (recommended: Windows 10 or Mac OSX 10.13 or higher) and a stable broadband Internet connection (cable modem, DSL, satellite broadband, etc., with a consistent 1.5 Mbps [megabits per second] download speed or higher. You can check your speed settings using the speed test on this website.)
6. **Late Work**: Late or incomplete work will be graded at 50% of the original point total.
7. **Technology in the Classroom**
   - Regarding electronic devices (such as laptops, tables, etc.), please be respectful of your peers and your instructor and do not engage in activities that are unrelated to class. Such disruptions show a lack of professionalism and may affect your participation grade. ***CELL PHONES AND OTHER COMMUNICATIVE DEVICES ARE NOT TO BE USED DURING CLASS UNLESS DESIGNATED BY THE INSTRUCTOR FOR CLASS PURPOSES***.
8. **Disability Accommodations**: Disability Services at George Mason University is committed to upholding the letter and spirit of the laws that ensure equal treatment of people with disabilities. Under the administration of University Life, Disability Services implements and coordinates reasonable accommodations and disability-related services that afford equal access to university programs and activities. Students can begin the registration process with Disability Services at any time during their enrollment at George Mason University. If you are seeking accommodations, please visit http://ds.gmu.edu/ for detailed information about the Disability Services registration process. Disability Services is located in Student Union Building I (SUB I), Suite 2500. Email:ods@gmu.edu | Phone: (703) 993-2474
9. **Covid-19 Note**: Students who have a Covid-related disability should contact the Disability Services office; DS will contact faculty using standard protocols about any students who require accommodations. Faculty are not expected to create accommodations for students outside of the Disability Services official guidelines.

10. **Diversity and Inclusion**: Students should be aware of support provided by the Center for Culture, Equity, and Empowerment and LBGTQ+. You can include (or link to) the Mason Non-Discrimination Policy or the Mason Diversity Statement, or include a statement like one of these:
    - Women and Gender Studies seeks to create a learning environment that fosters respect for people across identities. We welcome and value individuals and their differences, including gender expression and identity, race, economic status, sex, sexuality, ethnicity, national origin, first language, religion, age and ability. We encourage all members of the learning environment to engage with the material personally, but to also be open to exploring and learning from experiences different than their own.
    - The School of Integrative Studies, an intentionally inclusive community, promotes and maintains an equitable and just work and learning environment. We welcome and value individuals and their differences including race, economic status, gender expression and identity, sex, sexual orientation, ethnicity, national origin, first language, religion, age, and disability.
11. **Sexual Harassment, Sexual Misconduct, and Interpersonal Violence**:
    - We encourage students and employees who believe that they have been sexually harassed, sexually assaulted or subjected to sexual or interpersonal misconduct to seek assistance and support. University Policy 1202: Sexual Harassment and Misconduct speaks to the specifics of Mason's process, the resources, and the options available to students and employees.
    - Notice of mandatory reporting of sexual or interpersonal misconduct: As a faculty member, I am designated as a "Non-Confidential Employee," and must report all disclosures of sexual assault, sexual harassment, interpersonal violence, stalking, sexual exploitation, complicity, and retaliation to Mason's Title IX Coordinator per University Policy 1202. If you wish to speak with someone confidentially, please contact one of Mason's confidential resources, such as Student Support and Advocacy Center (SSAC) at 703-993-3686 or Counseling and Psychological Services (CAPS) at 703-993-2380. You may also seek assistance or support measures from Mason's Title IX Coordinator by calling 703-993-8730, or emailing titleix@gmu.edu.
12. **Privacy, Recording, and Sharing**:
    - Student privacy is governed by the Family Educational Rights and Privacy Act (FERPA) and is an essential aspect of any course.
    - Students must use their Mason email account to receive important University information, including communications related to this class. I will not respond to messages sent from or send messages to a non-Mason email address.

- Sharing of materials may be limited by what those materials contain and where they are shared:
    i. Sharing of class materials that contain identifiable student information is limited by FERPA .
    ii. Sharing of instructor-created materials, particularly materials relevant to assignments or exams, to public online "study" sites is considered a violation of Mason's Honor Code. For more information, see the Office of Academic Integrity's summary of information about online study sites. They also have a short video you can share with students or embed in your Blackboard course.

13. **Religious Holidays and Observations**: A reasonable effort will be made to allow students to observe their religious holidays consistent with class attendance policies stated in the syllabus, to make up the missed work. To receive this effort, students must provide prior notification to the instructor about dates/times as pertains to specific observances.
14. **Make–Up Policy**: This applies to presentations, reflection papers and exams. If a student has a university-approved excuse, you must notify me in writing prior. The allowance of such arrangements remains at the discretion of your instructor.
15. **Alteration of the Syllabus**: The instructor reserves the right to revise or amend this syllabus. Should any alterations be made, students will be notified via e-mail and in-class.

COURSE TEXT:

- *Definitive Guide to Cyber Threat Intelligence, Using Knowledge about Adversaries to Win the War against Targeted Attacks, Friedman, Jon., Bouchard, Mark. 2015*
- *Recorded Future: The Intelligence Handbook, Fourth Edition, A Roadmap for Building an Intelligence-Led Security Program, Ahlberg, Christopher, Ph.D., 2023*

GRADING CRITERIA: In this class you will be assessed based on the following:

- Midterm Exam (In-Person) (30%)
- Final Exam (In-Person) (30%)
- Group Project (30%)
- Class Participation & Discussion (10%)

GRADING SCALE:

- A+ 97 – 100%
- A 96 – 94%
- A- 93 – 90%
- B+ 89 – 87%

- B 86 – 84%
- B- 83 – 80%
- C+ 79 – 77%
- C 76 – 74%
- C- 73 – 70%
- D 69 – 67%
- D 66 – 64%
- D- 63 – 60%
- F Below 60%

TESTS, ASSIGNMENTS, PARTICIPATION, & PROJECTS:

- **Mid-Term Exam**: You will have a mid-term exam which covers topics from the first half of the semester. The exam will be in-person on Wednesday, February 28th from 07:20 – 10:00pm ET.
- **Final Exam**: You will have a final exam which covers topics from the entire semester. The exam will be in-person on Wednesday, May 1st from 07:20 – 10:00pm ET.
- **Group Project**: You will have a singular group project that will culminate with an in-class presentation and accompanying report during the semester. Each presentation will be based on teams, and you will be divided into your groups during the first week of classes.
    - ***Team Leaders***: Once you are divided into your teams for the semester, I will allow you time to meet, exchange contact information, and assign a team leader. The team leaders will contact me with any questions or concerns as you work on your projects. They will also be very useful in getting everyone together to work on the project. In addition, the team leader will gather feedback for each project/presentation (including how each team member contributed to be project).
- **Participation**:
    - This is an interactive, project-based course with significant group work. You must be prepared to work in a team during the semester. I expect students to be engaged during each class session, meaning being attentive to lectures with ideas, comments, and questions so that you may actively participate in the discussions.
    - It also means respectfully responding to the ideas and perspectives of your classmates, even if you may disagree with them.

- This course includes collaborative practices, such as teamwork on certain projects involving group engagement and preparation. ***<u>**Note that missed attendance without documentation during in-class presentations will result in a non-negotiable 10% impact on your final grade**</u>***.

COURSE SCHEDULE:

- **Week 1 ((Jan. 17th): Introduction to Cyber Threat Intelligence**
  - Overview of the course objectives and structure
  - Exploration of fundamental concepts and principles in cyber threat intelligence
  - Understanding the role of cyber threat intelligence in the realm of cybersecurity
  - Overview of CTI Group Project
- **Week 2 (Jan. 24th): Intelligence Data Sources and Collection**
  - Detailed examination of various intelligence data sources, including OSINT, HUMINT, SIGINT, and more
  - In-depth discussion of methodologies and techniques for systematic intelligence data collection
  - Ethical considerations and responsible practices in gathering intelligence data.
- **Week 3 (Jan. 31st): Intelligence Analysis and Interpretation**
  - Advanced techniques for analyzing and interpreting complex intelligence data.
  - Deep dive into analytical tools and frameworks employed in cyber threat intelligence.
  - Case studies highlight effective intelligence analysis and interpretation strategies.
- **Week 4 (Feb. 7th): Threat Actor Identification and Assessment**
  - Comprehensive exploration of different types of cyber threats, such as malware, phishing, and DDoS attacks
  - Methodical approaches for identifying, assessing, and categorizing cyber threats.
  - Introduction to the concept of threat modeling and its practical applications
- **Week 5 (Feb. 14th): Cyber Risk Mitigation Strategies**
  - Proactive strategies and best practices for mitigating diverse cyber risks.
  - In-depth analysis of incident response planning and management
  - Navigating regulatory compliance requirements and their influence on risk mitigation
  - Provide summary of CTI Group Project
- **Week 6 (Feb. 21st): Emerging Technologies and Their Impact on Cyber Threat Intelligence**

- Evaluation of the role of machine learning and artificial intelligence in shaping cyber threat intelligence practices
- Exploration of automation and orchestration techniques and their potential benefits in threat intelligence
- Real-world case studies showcasing the practical application of emerging technologies.

- **Week 7 (Feb. 28th): Midterm Test**
  - Cumulative mid-term exam assessing students' understanding of course content and concepts.
  - Integration of knowledge from all course topics
- ***Spring Break – No Classes between March 4 – 10th***
- **Week 8 (March 13th): Case Studies in Cyber Threat Intelligence**
  - In-depth analysis of real-world case studies illustrating cyber threat intelligence challenges and successes
  - Identification of key takeaways and lessons from notable cyber threat incidents
- **Week 9 (March 20th): Hands-on Exercises in Threat Intelligence**
  - Engaging practical exercises and simulations to reinforce threat intelligence analysis techniques.
  - Application of intelligence data interpretation skills in simulated scenarios
- **Week 10 (March 27th): Insider Threat Intelligence**
  - Define insider threats and distinguish intentional vs. unintentional actions.
  - Examine real-world examples to illustrate the diversity of insider threats.
  - Outline incident response protocols for investigating, containing, and recovering from insider incidents
- **Week 11 (April 3rd): VIP & Executive Protection Threat Intelligence**
  - Provide an overview of the unique security challenges associated with VIPs and executives.
  - Explore the importance of threat intelligence in safeguarding high-profile individuals and the organizations they represent.
  - Discuss methodologies for conducting risk assessments specific to VIPs and executives.
  - Cover intelligence gathering techniques, emphasizing the need for timely and accurate information to anticipate and mitigate potential threats.
- **Week 12 (April 10th) Cyber Fusion Center & Executive Communication**
  - Explore the role and functions of a Cyber Fusion Center in consolidating and analyzing diverse cybersecurity data.

- Discuss the importance of integrating threat intelligence, security analytics, and incident response within a Cyber Fusion Center for a comprehensive cybersecurity approach.
- Examine effective communication strategies tailored for executives within a Cyber Fusion Center context.
- Address techniques for translating technical information into business language, emphasizing the significance of conveying cybersecurity insights to support executive decision-making.

- **Week 13 (April 17th): Project Presentations**
  - In a culmination of the course with a comprehensive synthesis of acquired knowledge and skills, students showcase and present their comprehensive threat intelligence projects.
  - Peer evaluation and constructive feedback on project presentations
- **Week 14 (April 24th): Project Presentations Continued & Review for Final Exam**
  - If necessary, complete remaining project presentations.
  - Comprehensive review of course materials, concepts, and key takeaways
  - Preparation for the upcoming final exam through practice questions and collaborative discussions
- **Week 15 (May 1st): Final Exam**
  - Cumulative final exam assessing students' understanding of course content and concepts.
  - Integration of knowledge from all course topics