BIOD 610-DL1 Introduction to Cyber Warfare (Fall 2020)

Professor: Brian M. Mazanec, PhD
804-514-7317, brianmazanec@gmail.com
Virtual Office Hours: Tuesdays 7-8pm (EST) or by appointment.

Course Description: This course addresses emerging international relations, policy, doctrine, strategy, and operational issues associated with Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE)—collectively referred to as cyber warfare. It provides students with a comprehensive perspective and enhances their knowledge of cyber warfare conducted by both state and non-state actors.

Course Objectives/Learning Outcomes: During this course, students will demonstrate an understanding of: 1) the evolution of cyber warfare and the basic characteristics and methods of CNA, CND, and CNE; 2) the current national policies, doctrines, and strategies relative to cyber warfare; and 3) the potential impact of cyber warfare on future international conflicts.

Course Schedule: The course will be taught during the fall 2019 term running from August 24, 2020 through December 5, 2020.

Required Reading: The following books are required reading.


All course materials, aside from the books identified above, will be available in the following Dropbox folder:
https://www.dropbox.com/sh/dljgdx0h5yvlc3u/AADn_sQBVhCLn-rQJdBNvkda?dl=0

Class Requirements and Structure:

Structure: This online course is divided into 14 learning modules. Each learning module contains a list of required reading, interactive discussion content for the module, and additional resources to help you learn the material. You must complete the activities for each module before the due date for the module listed on the calendar. You may work ahead on the modules, but will not receive feedback on your work until after the due date.
has passed. You must submit the analytic policy memo and research paper by the due dates specified in the syllabus.

**Participation and Attendance:** Regular and active participation is an essential, unmistakably important aspect of this online course. It is critical that students read all of the assigned material as well as all of the interactive discussion content. Your full participation on a regular basis is not only a requirement; it is an essential aspect of the online course process.

**Learning Activities:** There will be a learning activity during each module in the form of discussion questions. Students must post a comment in response to both discussion questions by the module due date listed in the syllabus and also must regularly respond (to at least one other students’ comments) in order to foster a dialogue on the particular topic. Comments should reflect that the student has done the assigned reading for the module. Being part of a learning community is an important part of an online class. While no group work is assigned in this course, you are expected to communicate about cyber issues with the other members of the class through the learning modules. Learning Activity participation will be graded for each module and are worth a maximum of 10 points each, for a total of 140 points.

**Discussion Leaders:** In addition, students must sign up (via the discussion board setup for this purpose during the first week of the course) to be a discussion leader for one learning module during the course, beginning with module three. There will be a limited number of discussion leaders for each learning module and assignments are on a first-come, first-serve basis. During the module when a student is serving as a discussion leader, in addition to participating in the regular learning activity, they should post a response to the following:

> What is the most important or interesting cybersecurity story in the news in the last week? What advice would you offer to the relevant leaders and policymakers related to the story?

Discussion leader participation will be graded and is worth a maximum of 20 points.

**Analytic Policy Memo:** Students will write an analytic policy memo addressed to the National Security Council’s Cybersecurity Coordinator regarding a specific scenario assigned during the course. This memo should be between 1,000-1,500 words in length and directly address the policy issues presented in the scenario, identify options, and offer specific recommendations. For details on how to write a policy memo, see Dr. Thrall’s instructions (posted in the Resources folder on Blackboard, under course content). The Analytic Policy Memo will be worth a maximum of 75 points and it should be emailed to the instructor in PDF format by the due date listed in this syllabus.

**Student names should be included in the PDF file name and on the first page along with the total word count.** Policy memos will be shared with the entire class and students will comment on each other’s memos in a later session.

**Research Paper:** Students will write an approximately 4,000-word (15 pages, double spaced) research paper on an approved topic of their choice related to CNA and/or CNE. Students should email the instructor before module three is due with a proposed topic for approval. The research paper will be worth a maximum of 200 points and
should be emailed to the instructor in PDF format by the due date listed in this syllabus. **Student names should be included in the PDF file name and on the first page along with the total word count and a short abstract.**

**Grading:** There will be 435 total points in this course (75 for the analytic policy memo, 200 for the research paper, 140 for regular learning activities, and 20 for discussion leader participation). There is no extra credit offered in this course.

**University Policies and Information:**

**Academic Integrity:** Faculty in the Schar School have zero tolerance for academic dishonesty and will strictly enforce Mason’s honor code.

**Disabilities:** If you are a student with a disability and you need academic accommodations, please see me and contact the Disability Resource Center (DRC) at 993-2474. All academic accommodations must be arranged through the DRC.

**Email:** Mason uses only Mason email accounts to communicate with enrolled students. Students must activate their Mason email account, use it to communicate with their department and other administrative units, and check it regularly for important university information including messages related to this class.

**University Catalog**, [http://catalog.gmu.edu](http://catalog.gmu.edu), is the central resource for university policies affecting student, faculty, and staff conduct in university academic affairs. Other policies are available at [http://universitypolicy.gmu.edu/](http://universitypolicy.gmu.edu/). All members of the university community are responsible for knowing and following established policies.

**Late Work:** The deadlines for the learning activities, analytic policy memo, and research paper are strict and extensions will not be permitted in the absence of a genuine emergency or documented illness. A late submission will be penalized a full letter grade (for example, from A to B) for every 24-hour period that it is late.

**Syllabus and Course Changes:** The syllabus is a general plan for the course. Deviations may be necessary and will be announced by me. The most likely changes will be to dates on the schedule. This syllabus is not a contract and is subject to change at the sole discretion of the instructor.

**Course Outline/Modules:**

**Part One: Introduction to Cyberspace and Cyber Warfare (Offense, Defense, and**

**Module One, due August 27, 2020:** **Class Introductions and Overview**

- **Readings:**
  - **Books:** Whyte and Mazanec, chapter 1
  - **Articles:** Course syllabus

- **Learning Activity:**
In the discussion board, post an introduction of yourself, discussing 1) your background, and 2) what you hope to get out of this course/why you are taking this course.

Consider what module you would like to sign up to serve as a discussion leader and sign up before the end of the first week.

To maintain situational awareness of cyber current events during the course (and after, if you wish), subscribe to:

- Bruce Schneier’s Crypto-Gram, here: https://www.schneier.com/crypto-gram/

Module Two, due September 3, 2020: **Introduction to the Cyberspace Domain and Cyber Conflict**

- **Readings:**
  - **Books:** Blum, chapters 1-3; Whyte and Mazanec, chapters 2 and 3
  - **Articles:** Clark, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, chapter 2 (p. 12); Kaspersky, *Navigating the Threat Landscape*; Naughton, *The Evolution of the Internet: From Military Experiment to General Purpose Technology*, DHS, NCCIC Cyber Incident Scoring System

- **Videos:** Confidentiality, Integrity, and Availability of Computer Security Overview, found here: https://www.youtube.com/watch?v=j8FT9WqmuDY

- **Interactive/Internet (optional):** NSA Archive Cyber Glossary: https://nsarchive.gwu.edu/news/cyber-vault/2018-09-19/cyber-glossary

- **Learning Activity:** In the discussion board, respond to the following:
  - How did the history of the Internet’s formation shape its security concerns today?
  - In what ways is cyberspace analogous to the “natural” physical domains of land, sea, air, and water? In what ways is it different?

Module Three, due September 10, 2020: **Computer Network Exploitation and Cyber Crime**

- **Readings:**
  - **Books:** Blum, chapters 4-7; Whyte and Mazanec, chapter 4

- **Videos:** FBI-produced video on Solar Sunrise, found here: http://www.youtube.com/watch?feature=player_embedded&v=bQr5CtgYnsA

- **Interactive/Internet (optional):** Kaspersky Real Time Cyber Threat Map, found here: http://cybermap.kaspersky.com/

- **Learning Activity:** In the discussion board, respond to the following:
o Is it important to distinguish between different types of cyber attacks? How should we do it?

o What risk, if any, do breakthroughs in quantum computing, neuromorphic computing, etc. pose to modern cryptography as an effective method to defend against CNE?

Module Four, due September 17, 2020: **Computer Network Attack**

- **Readings:**
  - Books: Blum, epilogue; Whyte and Mazanec, chapter 5

- Videos: Ralph Langner’s Stuxnet TED Talk, found here: [http://www.youtube.com/watch?v=CS01Hmjv1pQ](http://www.youtube.com/watch?v=CS01Hmjv1pQ).


- Learning Activity: In the discussion board, respond to the following:
  - Is cyberspace at risk of being “militarized”?
  - Is CNA properly categorized as a form of warfare/armed conflict or sabotage/clandestine action? Why does the answer matter?

Module Five, due September 24, 2020: **Computer Network Defense and Response**

- **Readings:**
  - Books: Whyte and Mazanec, chapter 6
  - Articles: Slayton, *What is the Cyber Offense-Defense Balance*, The White House, *Fact Sheet on Cybersecurity National Action Plan*; Clark, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, sections 3.3 (p. 23), 4.1.3 (p. 38), and 4.2.5 (p. 59); and Bryant, *Resiliency in Future Cyber Combat*; GAO GAO-18-645T (highlights page);

- Learning Activity: In the discussion board, respond to the following:
  - What is the greatest challenge facing the United States in defending against cyber attacks, and why?
  - Where does the responsibility of private firms begin and end in cybersecurity?

Module Six, due October 1, 2020: **Cyber Deterrence**

- **Readings:**
  - Books: Whyte and Mazanec, chapter 7
  - Articles: and Lindsay, *Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence against Cyberattack*, Poznansky, *Did the U.S. ‘hack back’ at Russia? Here’s why this matters in cyberwarfare*; Bebber, *There is No Such Thing as Cyber Deterrence. Please Stop*; and Joint Forces Quarterly interview with Pail Nakasone (p. 10-15)

- Learning Activity: In the discussion board, respond to the following:
  - What kind of cyber attacks, if any, can be reliably deterred, and why?
What will be the greatest impact on international relations of the fact that cyberspace appears to be offense-dominant?

Part Two: State-Based Cyber Warfare

Module Seven, due October 8, 2020: U.S. and Israeli Cyber Warfare

- Readings:
  - Books: Whyte and Mazanec, chapter 10, p. 205-225
- Learning Activity: In the discussion board, respond to the following:
  - What are the implications of the U.S.’s shift to focus on persistent engagement in cyberspace and why did it pursue this new approach?
  - What can the United States learn from Israel’s approach to cyber warfare?

Module Eight, due October 15, 2020: Chinese and Russian Cyber Warfare

- Readings:
  - Books: Whyte and Mazanec, chapter 10, p. 225-235
  - Articles: Mandiant, APT1 Report (p.1-6); ICA 2017-01D: Assessing Russian Activities and Intentions in Recent US Elections; DOD, Annual Report to Congress on Chinese Power (executive summary); Zetter, Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid; Lindsay, The Impact of China on Cybersecurity; Segal, When China Rules the Web; ; Crowdstrike, Global Threat Report 2020 (p. 51-60); and Libicki, The Convergence of Information Warfare
- Learning Activity: In the discussion board, respond to the following:
  - How might China use cyber weapons should a conflict with the U.S. occur over the South China Sea or Taiwan?
  - What does Russia’s use of cyber operations alongside physical operations in Georgia and Ukraine signal for the future of cyber warfare?

Module Nine, due October 22, 2020: Iranian and North Korean Cyber Warfare

- Readings:
  - Books: Whyte and Mazanec, chapter 10, p. 235-244
  - Articles: FireEye, APT38, Un-usual Suspects; Carnegie, Iran’s Cyber Threat: Espionage, Sabotage, and Revenge (timeline, summary, and introduction) Berman, The Iranian Cyber Threat, Revisited; Connell, Deterring Iran’s Use of Offensive Cyber; CSIS, Executive Summary of North Korea’s Cyber Operations: Strategy and Responses; Crowdstrike,
Global Threat Report 2020 (p. 40-50); and HP, Profiling an Enigma: The Mystery of North Korea’s Cyber Threat Landscape (p. 10-41)

- Learning Activity: In the discussion board, respond to the following:
  - What does Iran and North Korea’s development of sophisticated cyber capabilities portend for the international diffusion of cyber weapons?
  - Had the United States and/or Israel not allegedly engaged in CNA operations against Iran (e.g. Stuxnet), would Iran have still have developed its cyber capabilities?

Module Ten, due October 29, 2020: Ethics, Norms, and International Law for Cyber Warfare

- Readings:
  - Books: Whyte and Mazanec, chapter 11
  - Articles: NATO, The Tallinn Manual (introduction, p.1-11); Atlantic Council, Tallinn Manual Fact Sheet; The White House, The International Strategy for Cyberspace (p.9-11); Schmitt, International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed; Clark, At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues, section 5.4.3 (p. 71); Rabkin, To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict; Osula et. al, International Cyber Norms (introduction); Bing, Trump administration says China broke Obama-Xi hacking agreement

- Learning Activity: In the discussion board, respond to the following:
  - Should the U.S. unilaterally disavow offensive certain cyber weapons (as President Nixon did with offensive biological weapons) in order to promote a norm against possessing or using such weapons?
  - Would using ISPs to cut off/block all Internet traffic from a country and effectively enact a “cyber blockade” be an act of war in cyberspace?

- Analytic Policy Memo Due (emailed to instructor who will then upload/post in Module Eleven, per below)

Part Three: Non-State Cyber Warfare

Module Eleven, due November 5, 2020: Terrorism and Cyberspace

- Readings:
  - Books: Whyte and Mazanec, chapter 9
  - Articles: Rattray, Non-State Actors and Cyber Conflict (CNAS Cyber Volume 2, p.65-86); United Nations, The Use of the Internet for Terrorist Purposes, chapter 1 (p. 3-14); Theohary, Terrorist Use of the Internet: Information Operations in Cyberspace; CSIS, US Cyber Command Opening Up New Front Against ISIS; and Garrett, Taming the Wild Wild Web: 21st Century Prize Law and Privateers as a Solution to Combating Cyber Attacks

- Each students’ policy memos—to be posted by students concurrent with their submission to the instructor

- Learning Activity: In the discussion board, respond to the following:
  - What recommended options from your colleagues’ analytic policy memos did you find 1) most compelling and 2) least compelling? Please explain your rationale for each.
Why have terrorists not yet successfully conducted a major CNA-style attack in cyberspace?

Module Twelve, due November 12, 2020: Hackers and Social Activism

- Readings:
  - Books: Whyte and Mazanec, chapter 8
  - Articles: Casserly, What is Hacktivism? A short history of Anonymous, Lulzsec, and the Arab Spring; Denning, Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy (RAND, p. 239-288)

- Learning Activity: In the discussion board, respond to the following:
  - How do non-state actors use cyberspace to promote advocacy or achieve objectives? How is this activity evolving and where might it go in the future?
  - Can you truly be anonymous online? Should you be?

Part Four: The Future of Cyber Warfare


- Readings:
  - Books: Whyte and Mazanec, chapter 12

- Learning Activity: In the discussion board, respond to the following:
  - How, if at all, should the United States share identified zero-day vulnerabilities with private industry to mitigate the vulnerability?
  - Should the United States issue letters of marque and reprisal to authorize private persons (privateers) to “hack back” and attack and destroy bad actors in cyberspace?

Module Fourteen, due December 3, 2020: The Future of Cyber Warfare: International Dimensions

- Readings:
  - Books: None
  - Articles: Liff, Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War; Rid, More Attacks, Less Violence; Chapelée, Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation (executive summary); GAO, GAO-19-204SP; C4ISRNET, How 5G is the key to protecting US interests, and Forbes, Can AI Become Our New Cybersecurity Sheriff?

- Learning Activity: In the discussion board, respond to the following:
  - What are the emerging and future technologies that we will have to worry the most about from a security perspective?
  - Who will win the fight for the future of 5G and why does this matter?
Research Paper Due – December 4, 2020