**INTA 4803**

**Cyber Warfare: *A Domestic Issue***

**Logistics:**

Fall 2018

3 Credits

Thursdays 3:00 – 5:45 PM

Ivan Allen College (Habersham) G-17

**Prerequisites:**

None

**Instructor:**

Holly M. Dragoo

**Office:**

Centennial Research Building

400 10th St. NE #319

Atlanta, GA 30318

Phone: 404-407-7573

*For appointments only\**

Campus Location: Habersham Basement Computer Lab/Student Lounge

Hours: 12:30 – 2:30 PM Thursdays

or by appointment

**Required Materials:**

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld* ***2nd Edition***. O'Reilly Media, Inc., 2011. ISBN: 978-1-449-31004-2

Kaplan, Frank. *Dark Territory: The Secret History of Cyber War.* Simon & Schuster, Inc., 2016.

ISBN: 978-1476763262

**Overview:**

This class intends to give students a broad overview of the nature of conflict and national security aspects of cyberspace. This includes, but is not limited to, cyber warfare and intelligence gathering activities, domestic policies pertaining to cyberspace, the difference between cyber terrorism and cybercrime, and how the U.S. government responds to cyberattacks. Students should take away from the class an appreciation for the complexity and ambiguity surrounding cyber events and the key stakeholders involved in cybersecurity policymaking and response to said events. This class is intended to be a compliment to Cybersecurity in International Relations (INTA 4803).

**Learning Objectives:**

1. Demonstrate briefing skills and focus on clearly conveying complex concepts in simple, concise ways.
2. Practice word economy and strategic editing skills in writing a series of policy memos.
3. Describe the OSI model and discern when policies cover specific parts of it.
4. Identify key stakeholders in the U.S. government in cyber policy and cyber event response.
5. Compare and contrast the differences between acts of war, acts of aggression, intelligence activities, terrorism, and crime in cyberspace.
6. Present arguments for policies surrounding the privacy vs. security dilemma.
7. Apply concepts in an analytic simulation designed to replicate actual official responses by different actors to a cyber event.

**Class Requirements:**

1. Attendance & Participation (15%)
2. Policy Memos (35%)
	1. 2-3pg. each (3)
	2. Final policy assessment (1)
3. Oral Briefings (15%)
	1. Stand-up brief (2)
4. Cyber Event Response Simulation (35%)
	1. Participation/Teamwork
	2. Group Presentation

**Assignments:**

All assignments will be due electronically by 3 PM on Thursdays.

*Assignments and guidance will be distributed separately and in class.*

**Attendance & Participation:**

You are expected to be in class every day, on time. If you know of a potential conflict that will prevent you from attending class, please make arrangements with a classmate to go over the missed content or see the instructor.

*\*We only meet once a week – if you miss one class, you will be behind one week, not one class.\**

**Academic Integrity:**

Each student enrolled at GT signed the Georgia Tech Honor Code before attending classes. You will be held to this standard, understanding that violations will be reported to the Dean of Students and the Office of Student Integrity (OSI) for investigation.

For more information on the Honor Code and ethics at Georgia Tech, please visit: <http://osi.gatech.edu/>

<https://policylibrary.gatech.edu/student-affairs/academic-honor-code>

**Additional Notes:**

Special accommodation for students with documented disabilities can be made through the ADAPTS office – please notify the instructor as early as possible if this applies to you.

**THIS SYLLABUS IS A LIVING DOCUMENT AND IS SUBJECT TO CHANGES**

**THROUGHOUT THE SEMESTER**

**Course Calendar:**

**WEEK 1 – Aug 23 Overview, Definitions + Who Governs Cyberspace?**

* Introductions & housekeeping
* Scope of the class & organization
* Computer science vocabulary & OSI Model review
* Course content overview

Readings:

1. Carr, pp. 263-273
2. Carter, Ash. "The DOD cyber strategy." *Defense News.* 2015. <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf>
3. "Cyberwar Threat | NOVA | PBS". 2018. *PBS*. Accessed January 3 2018. <http://www.pbs.org/video/nova-cyberwar-threat-pro/>

**WEEK 2 – Aug 30 Threats in Cyberspace**

Class time will be spent completing the group activity on OSI Model layers and Assignment #1 group paper.

*\*\*\*Assignments must have ALL GROUP MEMBER NAMES on it and is due by 5 PM on FRI 31 AUG*

Readings:

1. Carr, pp. 141-159
2. Kaplan, pp. 107-143
3. US Committee on Armed Services. “Foreign Cyber Threats to the United States”. January 2017. *Armed-Services.Senate.Gov*. <https://www.armed-services.senate.gov/hearings/17-01-05-foreign-cyber-threats-to-the-united-states>
4. <https://www.lifewire.com/open-systems-interconnection-model-816290>
5. <https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017>

**WEEK 3 – Sep 6 Deterrence in Cyberspace**

\*\*\*Guest Lecture – Professor Salamone\*\*\*

Watch in class: https://www.defense.gov/News/Special-Reports/0218\_npr/

Readings:

1. Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009. Appendix B – The Calculus of Explicit vs. Implicit Deterrence pp. 183-197 <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf>
2. Gartzke, Erik, and Jon R. Lindsay. "Thermonuclear Cyberwar." *Journal of Cybersecurity* 3, no. 1 (2017): 37-48. <https://academic.oup.com/cybersecurity/article/3/1/37/2996537>
3. Herzinger, Blake D. “Cyber Secrecy Undermines Deterrence”. September 2016. *Proceedings Magazine*. Vol. 142/9/1363. <https://www.usni.org/magazines/proceedings/2016-09/cyber-secrecy-undermines-deterrence>

**WEEK 4 – Sep 13 Cyber Warfare**

*\*\*\*First policy memo due at 3 PM on THURS 13 SEPT.*

Readings:

1. Carr, pp. 31-75
2. Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009. Appendix A – What Constitutes an Act of War in Cyberspace? pp. 179-181 <https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf>
3. Caton, Jeffrey L. *Distinguishing Acts of War in Cyberspace: Assessment Criteria, Policy Considerations, and Response Implications.* Army War College Carlisle Barracks, PA Strategic Studies Institute, 2014. **Pp. 1-33.** <https://ssi.armywarcollege.edu/pdffiles/PUB1229.pdf>
4. Franzese, Patrick W. "Sovereignty in Cyberspace: Can it exist." *AFL rev.* 64 (2009). Pp. 7-17. <http://heinonline.org/HOL/Page?handle=hein.journals/airfor64&div=4&g_sent=1&casa_token=&collection=journals>

**WEEK 5 – Sep 20 The Attribution Problem**

Readings:

1. Carr, pp. 131-140
2. Erik M. Mudrinich, "Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and the Attribution Problem," *Air Force Law Review* 68 (2012). Pp. 187- 205 <http://heinonline.org/HOL/Page?handle=hein.journals/airfor68&div=7&g_sent=1&casa_token=&collection=journals>
3. Healey, Jason. *Beyond attribution: Seeking national responsibility for cyberattacks.* Atlantic Council of the United States, 2012. <http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF>
4. Knake, Robert K. "Untangling attribution: Moving to accountability in cyberspace." *Prepared Statement before the Subcommittee on Technology and Innovation, Committee on Science and Technology, Hearing: Planning for the Future of Cyber Attack* (2010). Pp. 1-12 <https://www.cfr.org/sites/default/files/pdf/2010/07/Knake%20-Testimony%20071510.pdf>

**WEEK 6 – Sep 27 Active Defense Strategies**

Readings:

1. Carr, pp. 273-283
2. Johnson, J. “Implementing Active Defense Systems on Private Networks”. August 2013. *Sans.org.* <https://www.sans.org/reading-room/whitepapers/detection/implementing-active-defense-systems-private-networks-34312>
3. Glosson, Anthony D. "Active Defense: An Overview of the Debate and a Way Forward." 2015. *Mercatus.org.* <https://www.mercatus.org/system/files/Glosson-Active-Defense.pdf>

**WEEK 7 – Oct 4 Intelligence Operations in Cyberspace**

Readings:

1. Carr, pp. 77-89
2. Kaplan, pp. 221-236
3. Warner, Michael. 2018. "Intelligence in Cyber—And Cyber in Intelligence - Understanding Cyber Conflict: 14 Analogies". *Carnegie Endowment for International Peace*. <http://carnegieendowment.org/2017/10/16/intelligence-in-cyber-and-cyber-in-intelligence-pub-73393>
4. Lin, Herbert S. "Offensive cyber operations and the use of force." *Journal of National Security, Law & Policy* 4; 2010. Pp. 63-86. <http://jnslp.com/wp-content/uploads/2010/08/06_Lin.pdf>

**WEEK 8-10 – Oct 11-25 Analytic Simulation & Cyber Event Response**

*\*\*\*Second policy memo due at 3 PM on THURS 11 OCT.*

Readings:

1. Carr, pp. 263-271
2. Kaplan, pp. 171-189
3. Caton, pp. 48-75
4. Government Accountability Office, U.S. 2016. "Civil Support: DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities During Cyber Incidents". *Gao.Gov*. <https://www.gao.gov/assets/680/676322.pdf>

**WEEK 11 – Nov 1 Privacy vs. Security Part 1**

Readings:

#### Kaplan, pp. 237-264

#### "FISA Section 702: Is Warrantless Surveillance National Security or A Hit to Privacy?". 2018. *McClatchy*. <http://www.mcclatchydc.com/news/politics-government/congress/article135841918.html>

#### Kris, David. "Don't Read Too Much Into The Jump In Rejected FISA Applications". 2018. *Lawfare*. <https://www.lawfareblog.com/dont-read-too-much-jump-rejected-fisa-applications>.

#### U.S. Office of National Intelligence. “FISA Amendments Act Q&A” 2017. *Dni.Gov*. <https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf>

#### U.S. Office of National Intelligence. “Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act." 2018. *IC ON THE RECORD*. <https://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of>

**WEEK 12 – Nov 8 Privacy vs. Security Part 2**

*\*\*\*Third policy memo due at 3 PM on THURSDAY 8 NOV.*

Readings:

#### Supreme Court of the U.S. "Carpenter V. United States - Scotusblog". 2018. *Scotusblog*.

#### <http://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/>

#### Transcript found here: <https://www.supremecourt.gov/oral_arguments/argument_transcripts/2017/16-402_3f14.pdf>

#### Summary found here:

#### “Carpenter v. United States." Oyez. <https://www.oyez.org/cases/2017/16-402>.

#### Howe, Amy. “Argument analysis: Drawing a line on privacy for cell phone records, but where?” SCOTUSblog. 29 November 2017. <http://www.scotusblog.com/2017/11/argument-analysis-drawing-line-privacy-cellphone-records/>

1. "Katz V. United States, 389 U.S. 347 (1967)". 2018. *Justia Law*. Accessed May 29 2018. <https://supreme.justia.com/cases/federal/us/389/347/>
2. "Olmstead V. United States, 277 U.S. 438 (1928)". 2018. *Justia Law*. <https://supreme.justia.com/cases/federal/us/277/438/>
3. "Smith V. Maryland, 442 U.S. 735 (1979)". 2018. *Justia Law*. <https://supreme.justia.com/cases/federal/us/442/735/>

#### Eidam, Eyragon. "Privacy Vs. Security: Experts Debate Merits of Each in Tech-Rich World". 7 June 2017. *Govtech.Com*. <http://www.govtech.com/policy/Privacy-vs-Security-Experts-Debate-Merits-of-Each-in-Tech-Rich-World.html>.

**WEEK 13 – Nov 15**

**WEEK 14 – Nov 21-23 THANKSGIVING BREAK**

**WEEK 15 – Nov 29 Cybercrime vs. Cyber Terrorism + Wrap-up & Review**

Readings:

1. Carr, pp. 15-30, 89-102
2. Caton, pp. 42-49
3. Gilmour, Stan. "Policing crime and terrorism in cyberspace: An overview." *European Review of Organised Crime* 1, no. 1 (2014): 143-159. <https://s3.amazonaws.com/academia.edu.documents/34096828/EROC119.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1515170874&Signature=kDS6V7wZ4cT7bJrBZka0LZvaBak%3D&response-content-disposition=inline%3B%20filename%3DGilmour_Policing_Crime_and_Terrorism_in.pdf>
4. Holt, Thomas J. "Exploring the intersections of technology, crime, and terror." *Terrorism and Political Violence* 24, no. 2 (2012): 337-354. <http://www.tandfonline.com/doi/full/10.1080/09546553.2011.648350?scroll=top&needAccess=true#aHR0cDovL3d3dy50YW5kZm9ubGluZS5jb20vZG9pL3BkZi8xMC4xMDgwLzA5NTQ2NTUzLjIwMTEuNjQ4MzUwP25lZWRBY2Nlc3M9dHJ1ZUBAQDA>=
5. Rollins, John, and Clay Wilson. "Terrorist capabilities for cyberattack: Overview and Policy issues." 2007. <http://www.c4i.org/RL33123.pdf>

**IMPORTANT DATES**

* Thursday 29 November = Final Class
* Wednesday 5 December = Reading Period
* Thursday 6 December = **No Class**
* No Final Exam
* ***Final Papers Due Friday 7 December at NOON****.*