**INTA 4803**

**Cybersecurity: *A Global Issue***

**Logistics:**

Spring 2018

3 Credits

MWF 09:00 – 09:55 AM

Howey (Physics) S105A

**Prerequisites:**

None

**Instructor:**

Holly M. Dragoo

**Office:**

Main:

Wells Fargo Building, Atlantic Station

171 17th St. NW Ste. #950

Atlanta, GA 30363

Phone: 404-407-7573

*For appointments only\**

Campus Location: Habersham Basement Computer Lab/Student Lounge

Hours: 0900 – 1100 AM Tuesdays

or by appointment

**Materials:**

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

**Overview:**

This class intends to give students a broad overview of the nature of international relations and national security aspects of cyberspace. This includes, but is not limited to, cyber warfare and intelligence gathering activities, international agreements and domestic policies pertaining to cyberspace, the difference between cyber terrorism and cybercrime, and how governments respond 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 responding to said events.

**Learning Objectives:**

1. Demonstrate briefing skills and focus on clearly conveying complex concepts in simple ways.
2. Produce concise writing in a series of policy memos that will force strategic editing and word economy.
3. Describe the OSI model and discern when policies cover specific parts of it.
4. Identify key stakeholders in the US 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 (25%)
	1. 2-3pg. each (3)
	2. 5-6pg. policy assessment/final (1)
3. Oral Briefings (25%)
	1. Stand-up briefs (2)
	2. Simulation review
4. Cyber Event Response Simulation (35%)
	1. Participation/Teamwork
	2. Group Presentation

**Assignments:**

All assignments will be due electronically by NOON on Fridays.

*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 missed content or see the instructor.

**Academic Integrity:**

Each student 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 – Jan 8 – 12 Definitions & Overview**

*Friday 12 January = Last day to drop classes without penalty*

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

Readings:

1. Carr, pp. 1-15 (optional)
2. <https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017>
3. <https://www.lifewire.com/open-systems-interconnection-model-816290>

**WEEK 2 – Jan 17 – 19 Who Governs Cyberspace?**

*Monday 15 January – MLK Day =* ***No Class***

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. Lewis, James. "Piecemeal Measures Regulate Cyberspace". 26 September 2017. *The Cipher Brief*. <https://www.thecipherbrief.com/cyberspace-defies-international-regulation>
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 3 – Jan 22 – 26 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. 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://pdfs.semanticscholar.org/01ed/f0bb2f749d86b8fa67d9262c56bf83067415.pdf>

**WEEK 4 – Jan 29 – Feb 2 Threats in Cyberspace**

*\*\*\*First policy memo due at NOON on Friday 2 February.*

Readings:

1. Carr, pp. 141-159
2. "Cyberwar Threat | NOVA | PBS". 2018. *PBS*. Accessed January 3 2018. <http://www.pbs.org/video/nova-cyberwar-threat-pro/>
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>

**WEEK 5 – Feb 5 – 9 Cyber Warfare**

Readings:

1. Carr, pp. 31-75
2. 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>

**WEEK 6 – Feb 12 – 16 Intelligence Operations in Cyberspace**

Readings:

1. Carr, pp. 77-89
2. 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>
3. 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 7 – Feb 19 – 23 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 8 – Feb 26 – Mar 2 Deterrence in Cyberspace**

*\*\*\*Second policy memo due at NOON on Friday 2 March.*

Readings:

1. Libicki, Martin C. *Cyberdeterrence and cyberwar*. Rand Corporation, 2009.
	1. 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 9 – Mar 5 – 9 International Community**

Readings:

1. Sofaer, Abraham, David Clark, and Whitfield Diffie. "Cyber Security and International Agreements." In *National Research Council, Proceedings of a Workshop on Deterring Cyberattacks*. 2009. <https://www.nap.edu/read/12997/chapter/13#187>
2. Caton, pp. 34-42
3. Limnell, Jarno. "Can Finland Act as A Mediator on Cyber Norms?". 28 May 2015. *Council on Foreign Relations*. Accessed November 21 2017. <https://www.cfr.org/blog/can-finland-act-mediator-cyber-norms>
4. United Nations Institute for Disarmament Research (UNIDIR). *The Cyber Index: International Security Trends and Realities.* Geneva: UN, 2013.  Pp. 1-5, 91-112 <http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf>

**WEEK 10 – Mar 12 – 16 Nation-State Capabilities**

*Wednesday 14 March = Last day to withdraw or change grade mode*

Readings:

1. Carr, pp. 243-263
2. UNIDIR, pp. 9 - 90

**Mar 19 – 23 = SPRING BREAK**

**WEEK 11 – Mar 26 – 30 Analytic Simulation**

**WEEK 12 – Apr 2 – 6 Cyber Event Response**

*\*\*\*Third policy memo due at NOON on Friday 6 April.*

Readings:

1. Carr, pp. 45 – 75
2. Caton, pp. 48-75
3. 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>
4. US Strategic Command. “Strategic Command Directive (SD) 527-1: Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures”. 2006*. Info.publicIntelligence.net.* SD-527-1; Pp. 1-35. <https://info.publicintelligence.net/StrategicCommandDirective527-1_27JAN2006InformationOperationsCondition-INFOCON-System.pdf>
5. US Department of Defense (DoD). “Chairman of the Joint Chiefs of Staff Instruction: Information Assurance (IA) and Support to Computer Network Defense (CND)” 2015. *JCS.mil*. CJCSI 6510.01F; 1-114. <http://www.jcs.mil/Portals/36/Documents/Library/Instructions/6510_01.pdf?ver=2016-02-05-175054-497>

**WEEK 13 – Apr 9 – 13 Privacy vs. Security**

Readings:

#### 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>.

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

#### Bhatia, Gautam. 2015. "State Surveillance and The Right to Privacy in India: A Constitutional Biography". *Papers.Ssrn.Com*. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2605317>

#### 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>

**WEEK 14 – Apr 16 – 20 Cybercrime vs. Cyber Terrorism**

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>

**WEEK 15 – Apr 23 – 27 Wrap-up & Review**

* Monday 23 April = Final Class
* Wednesday 25 April = Reading Period
* Friday 27 April = **No Class**
* No Final Exam
* ***Final Papers Due Friday 4 May at NOON****.*