CISS 497A Cyber Warfare

Description

Cyber Space has joined air, land, sea and space as the latest domain of warfare. This course examines warfare in the cyber domain beginning with an understanding of how it fits within the context of traditional theory of war. The course examines how countries prepare and apply capabilities and strategies, the impacts of non-state actors, and the future development of cyber warfare. Students are prepared to understand the impact of the extension of warfare into the cyber domain.

Credits:	4 credit hours
Format:	Reading/Seminar
Prerequisite:	None
Suggested Textbooks:	Clarke, R. A., & Knake, R. (2012). *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY: Ecco. (ISBN: 9780061962240) Tzu, Sun.(5th Century BC). *The Art of War*. Trans. Lionel Giles http://classics.mit.edu/Tzu/artwar.html, Von Clauzwitz, Carl (1832). On War. Trans. James John Graham (1873). https://www.clausewitz.com/readings/OnWar1873/TOC.htm#TOC De Jomini, Baron. The Art of War, Trans Capt. G.H Mendell and Lieut. W.P. Craighill (1862). https://www.gutenberg.org/files/13549/13549-h/13549-h.htm
Assessment:	Papers, Presentations, Class participation

Student Learning Outcomes

On completion of this course, students will be able to:

- Evaluate the place of cyber warfare in the context of information warfare.
- Evaluate the impact of non-state actors on cyber warfare.
- Compare and contrast the cyber war strategies and capabilities of different countries.
- Assess cyber warfare in the context of the theory of war.
- Apply strategic thinking toward specific focused results.

Topics

- Analyze potential targets of cyber terrorists.
- Appraise how cyber warfare varies from traditional warfare.
- Appraise the capabilities needed for personnel engaged in various information warfare tasks.
- Assess the existence of boundaries between cyber and information warfare.
- Assess the impact of vigilantes, hacktivists, sympathetic hackers on crisis management and war termination.
- Assess the Order of Battle of nations with known cyber capabilities.
- Categorize the Anatomy of a Cyber Attack in military terms.
- Characterize what makes an attack an act of terrorism.
- Circumscribe the scope of cyber warfare.
- Compare and contrast how the variety of trans-state actors (jihadists, anarchists, political activists, criminal organizations, etc) differ in their approaches to the possibilities for cyberwar.
- Compare and contrast national cyber strategies.
- Compare and contrast the elements of information warfare engagement.
- Critique other proposals for treatment of cyber warfare.
- Critique traditional military approaches to information warfare capacities.
- Debate the merits of Cyber Treaties.
- Define the Spectrum of Conflict.
- Describe Chinese Cyber Strategy.
- Describe current use of Cyber Space by terrorists.
- Describe the evolving landscape of warfare.
- Describe the operational planning process.
- Describe the Russian Cyber Strategy.
- Describe the US Cyber Strategy.
- Differentiate between Acts of War and Acts Short of War.
- Differentiate between military and non-military cyber force components.
- Discuss proposals for Cyber Arms Controls.
- Discuss the 9 principles of war.
- Discuss the problem of attribution.
- Distinguish between State and Non-state actors.
- Evaluate relative advantages and disadvantages non-state actors have in developing capabilities.
- Evaluate the use of effects based planning.
- Evaluate what steps can reduce the threat of cyber terrorism.
- Explain Desired End State in terms of operational planning.
- Explore the possibility for cyberwarfare to increase the potential for failed states.
- Formulate what constitutes crossing the Kinetic Boundary.
- Investigate issues with the involvement of 3rd parties.
- Judge whether cyberwarfare provides impetus or significance to the emergence of new forms of conflict or protest.
- Outline Information Tasks and their intended effects.

- Outline known and potential offensive capabilities of cyber warfare participants.
- Outline the components of the US Cyber Command and their capabilities.
- Propose the ideal cyber force.
- Structure a vision the broader context of Information Warfare.
- Suggest how cyberwarfare influences approaches to peacekeeping and peacemaking.
- Understand basic theory of war.

Application of the Theory of War

The students will write a paper relating the Principles of War (von Clauswitz), The Art of War (Sun Tzu) or other traditional military theory to cyber warfare. The focus should include a limited scope of theory and how it can be applied or how it is refuted by the conditions of cyber warfare. The paper must include at least one example of actual cyber warfare activity.

The paper should be roughly 10 pages in length; should contain at least 3-5 references; and should be in proper format.

Country Assessment

Teams of students will complete an in-depth study of the cyber strategy and capabilities of an assigned country. The study should include inferred, as well as acknowledged, capabilities and strategies. The study should include a broad sketch of the overall defense/military posture, economic status, political situation, and foreign relations of the country.

Remember that military capabilities can be inferred from civilian capabilities. For example, countries which can produce cars and trucks for the civilian market are capable of producing vehicles for military use. "Programmers who program consumer products can program ..." All capabilities must be documented.

The students in the team will organize the team to cover the necessary information. Each student will be assigned at least one aspect for which they have sole responsibility. Some areas can be handled as joint responsibilities.

The results of the country assessment will be provided as a presentation. The students will arrange the format and details of delivery of the presentation with the instructor.

Application of Strategic Thinking to Cybersecurity

Based on their experience, students will prepare a presentation and paper reflecting on the application of strategic thinking to cybersecurity in the organization. Students will consider the impact of state and non-state actors on the future of cybersecurity and in how they will shape the cyber environment. Students should base their strategic thinking on current observed trends, as well as perceived future directions. As a part of their reflection, the students should propose specific concrete actions to be taken by businesses or other organizations in light of the strategic direction and relate those to warfare principles.

The presentation should be roughly 7 minutes in length and include specific references.

The paper should be roughly 10 pages in length; should contain at least 3-5 references; and should be in proper format.

Schedule

Week 1 & 2 – Classical Theory of War

Week 3 – Modern Theory of War

Week 4 – The Emergence of Cyber War – The China Paper

Week 5 – Modern Cyber War Strategy & Organization – US

Week 6 – Modern Cyber War Strategy & Organization – NATO, Russia, & Others

Week 7 – Applied Cyber Warfare – Ukraine, Stuxnet, etc.

Week 8 – Cyber Treaties and International Agreements

Week 9 – Non-state Actors

Week 10 – Cyber and Information Warfare

#	Day/ Date	Topic	Sub-topic(s)/Readings	Assignments
1	Wed 1/9	Introduction		
2	Fri 1/11	Classical War Theory - Ancient	*The Art of War* by Sun Tzu http://classics.mit.edu/Tzu/artwar.html	
3	Mon 1/14	Classical War Theory – Ancient	*Poliorketika* by Aeneas Tacticus http://www.aeneastacticus.net/public_html/text.htm *The Tactics of Aelian* by Tacticus Aelianus https://books.google.com.au/books/about/The_tactics_of_Aelian.html?id=6tITAAAAYAAJ Scan and select. Note: These were two different writers who lived about 100 years apart. **Extra Readings:** If you are interested in reading some Julius Caesar, his works (as well as many other classic writings) are available at: http://classics.mit.edu/ In particular his books on the Gallic Wars are at: http://classics.mit.edu/Caesar/gallic.html	

			Two other ancient writers worth reading are: Greek Historian - considered the Father of History: Herodotus. *Histories*. http://classics.mit.edu/Herodotus/history.html Roman Historian - Note the similarity of the names to the Greek strategists/tacticians: Tacitus. *The Annals.* http://classics.mit.edu/Tacitus/annals.html	
4	Wed 1/16	Classical War Theory – 19th Century	*On War*, by Karl Von Clausewitz, Book I & II https://www.clausewitz.com/readings/OnWar1873/TOC.htm **Optional:** A series of YouTube videos on the Wars of Napoleon. https://www.youtube.com/watch?v=s2z7iIsPLfE&list=PLaBYW76inbX41sSPLjvUyYfRY0B4ihYBN	
5	Fri 1/18	Classical War Theory – von Clausewitz	*On War*, by Karl Von Clausewitz, Book III &VIII https://www.clausewitz.com/readings/OnWar1873/TOC.htm Civil War Strategy 1861-1865 by Donald J. Stoker http://www.essentialcivilwarcurriculum.com/civil-war-strategy-1861-1865.html **Optional:** The Civil War Animated Map - https://www.battlefields.org/learn/maps/entire-civil-war-animated-map	
	Mon 1/21	**MLK Day**		
6	Wed 1/23	Classical War Theory – 19th Century	*The Art of War* by Baron De Jomini, Chpt I & II http://www.gutenberg.org/ebooks/13549 Clarke, Chpt 1	
7	Fri 1/25	Classical War Theory – 19th Century	*The Art of War* by Baron De Jomini, Chpt III & VII http://www.gutenberg.org/ebooks/13549 *The Influence of Sea Power Upon History, 1660-1783*, by A. T. Mahan. Introduction and Chapter 1. http://www.gutenberg.org/files/13529/13529-h/13529-h.htm	
8	Mon 1/28	Classical War Theory	Clarke, Chpt 2 *The Theory of Strategy* by B.H. Liddell Hart – files.	

		– 20th Century	*Strategy Maxims: 8 Lessons on Strategy from Sir. Basil H. Liddell-Hart* by Adam J. Doolittle. http://www.adamdoolittle.com/strategy-maxims/ **Recommended/Optional:** B. H. Liddell Hart, *Strategy 2nd Revised Ed.* - https://www.amazon.com/Strategy-Meridian-B-Liddell-Hart/dp/0452010713	
9	Wed 1/30	Modern Theory of War	JFSC Pub 1 Appendix D – See Files *THE EFFECTS-BASED APPROACH TO OPERATIONS* *http://www.doctrine.af.mil/Portals/61/documents/Annex_3-0/3-0-D06-OPS-EBAO.pdf* *http://www.businessinsider.com/ooda-loop-decision-making-2017-8* **Optional:** *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control by Berndt Brehmer* *http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf* *SCHOOLS FOR STRATEGY: TEACHING STRATEGY FOR 21ST CENTURY CONFLICT* by Colin S. Gray – See Files	
10	Fri 2/1	Modern Theory of War	Clarke, Chpt 3 *Cyber Power: A Personal Theory of Power* by Billy Pope - http://cimsec.org/cyber-power-personal-theory-power/11436 **Optional** *Cyberwar and B.H. Liddell Hart's Indirect Approach*, by Brandon Thomas Euhus – See Files, also https://www.hsdl.org/?view&did=813640	
11	Mon 2/4	China Cyber Strategy	*National Cyberspace Security Strategy (China)* https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/	
12	Wed 2/6	China Cyber Strategy	China Cyber Outlook https://www.csis.org/programs/technology-policy-program/technology-and-innovation/cybersecurity-and-governance/china Choose one article	
13	Fri 2/8		Clarke, Chpt 4	Theory Paper Due
14	Mon 2/11		National Cyber Strategy of the United States of America	

			https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf	
15	Wed 2/13	US Cyber Strategy	Joint Publication 3-12 Cyberspace Operations http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-06-19-092120-930 THE BEST STRATEGY FOR CYBER-CONFLICT MAY NOT BE A CYBER-STRATEGY - https://warontherocks.com/2016/11/the-best-strategy-for-cyber-conflict-may-not-be-a-cyber-strategy/ **Optional** *3 lessons the Army is taking from U.S. Cyber Command* by Mrk Pomerleau - https://myemail.constantcontact.com/3-lessons-the-Army-is-taking-from-U-S--Cyber-Command.html?soid=1114009586911&aid=RwIPkPKPv2Q	
16	Fri 2/15	Russian Cyber Strategy	Clarke, Chpt 5 Russia's Approach to Cyber Warfare https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf	
	Mon 2/18	**Presidents Day**		
17	Wed 2/20	County Analysis	Presentations	
18	Fri 2/22	Country Analysis	Presentations	
19	Mon 2/25		Clarke, Chpt 6	
20	Wed 2/27	Applied Cyber Warfare	Massive US-planned cyberattack against Iran went well beyond Stuxnet https://arstechnica.com/tech-policy/2016/02/massive-us-planned-cyberattack-against-iran-went-well-beyond-stuxnet/ Without Nuclear Deal, U.S. Expects Resurgence in Iranian Cyberattacks https://www.nytimes.com/2018/05/11/technology/iranian-hackers-united-states.html?rref=collection%2Ftimestopic%2FCyberwarfare&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=3&pgtype=collection	
21	Fri 3/1	Applied Cyber Warfare	Cyber Collateral Damage https://ac.els-cdn.com/S1877050916324590/1-s2.0-S1877050916324590-main.pdf?_tid=4c8a5928-939f-486d-8a99-	

			c633ce3c8ca3&acdnat=1520284122_086aec37fc0d2f674de7e10df4c36688 Cyber Warfare May Be Less Dangerous Than We Think https://www.washingtonpost.com/news/monkey-cage/wp/2018/04/26/what-can-cybergames-teach-us-about-cyberattacks-quite-a-lot-in-fact/?noredirect=on&utm_term=.00dd3bc1d516 Senate panel again looks to force Trump's hand on cyber warfare strategy. http://thehill.com/policy/cybersecurity/389381-senate-panel-again-looks-to-force-trumps-hand-on-cyber-warfare-strategy This cyberwar just got real. http://www.dw.com/en/this-cyberwar-just-got-real/a-43908697	
22	Mon 3/4	Cyber Treaties and International Agreements	States of cyber warfare: negotiating a cyber-weapons treaty - https://eandt.theiet.org/content/articles/2017/03/states-of-cyber-warfare-negotiating-a-cyber-weapons-treaty/ Putin on cyberwarfare: Action causes reaction, you don't like reaction - let's talk rules. https://www.rt.com/news/427709-putin-cybersecurity-rules-reaction/	
23	Wed 3/6	Non-state Actors	Clarke, Chpt 7 Computer Attack and Cyberterrorism - https://www.history.navy.mil/research/library/online-reading-room/title-list-alphabetically/c/computer-attack-cyberterrorism-crs.html The Cyber Terrorism Bogeyman - https://www.brookings.edu/articles/the-cyber-terror-bogeyman/ Two years for teen 'Cyber Terrorist' who targeted US officials - https://www.bbc.com/news/uk-england-leicestershire-43840075	
24	Fri 3/8	Cyber and Information Warfare	Why is Finland Able to Fend Off Putin's Information War? http://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/# THE NEW INFORMATION WARFARE - https://theintercept.com/2017/11/25/information-warfare-social-media-book-review-gaza/ **Optional:** Information Warfare in an Information Age http://ndupress.ndu.edu/Media/News/Article/1130649/information-warfare-in-an-information-age/ Coldwar 2.0: Russian Information Warfare https://globalsecurityreview.com/cold-war-2-0-russian-information-warfare/	

			FCC Chairman admits Russia Meddled in Net Neutrality Debate. https://www.engadget.com/2018/12/05/fcc-chairman-ajit-pai-russia-net-neutrality-comments/	
25	Mon 3/11	Cyber and Information Warfare	Clarke, Chpt 8 Modern Information Warfare Requires a New Intelligence Discipline - https://www.realcleardefense.com/articles/2018/02/20/modern_information_warfare_requires_new_intelligence_discipline_113081.html Respond to Russia's Information Warfare - https://www.usnews.com/opinion/world-report/articles/2017-07-17/the-us-needs-a-response-to-russias-information-warfare	
26	Wed 3/13		Strategic Thinking Presentations	
27	Fri 3/15		Strategic Thinking Presentations	