Lesson Plan: An Interdisciplinary Approach to Teaching Cyber Warfare Concepts

Donna M. Schaeffer, PhD Professor Marymount University

Patrick C. Olson Professor National University

This poster supports the idea that Cybersecurity, and thus cyber warfare are interdisciplinary topics. Based on the concepts that are covered from course descriptions on cyber warfare at various levels of study and from different disciplines, including computer science, criminal justice, and international relations the poster provides support for a single lesson plan on cyber warfare that includes learning competencies, recommended current materials, and easy to implement classroom activities. The lesson plan can be modified as needed for introducing the concepts of cyber warfare across disciplines.

Learning Objectives

After successfully completing this learning module, students will:

Be familiar with the historical emergence and evolution of cyber warfare

Be introduced to global perspectives and policies on cyber warfare

Be acquainted with cyber warfare capabilities of a selected nation-state

Required Reading

For Faculty Preparation:

Cyber Defense: An International Review (Giles & Hartmann, 2015). This book provides a survey of approaches by the German, Swedish, Norwegian, and Estonian defense organizations.

The Emerging Risk of Virtual Societal Warfare (Mazarr, Bauer, Casey, Heintz, & Matthews, 2019), a recent report from Rand Corporation. Available at https://www.rand.org/pubs/research_reports/RR2714.html

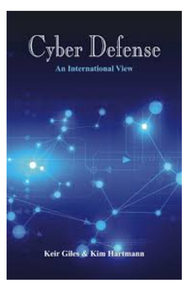
For Students (select from):

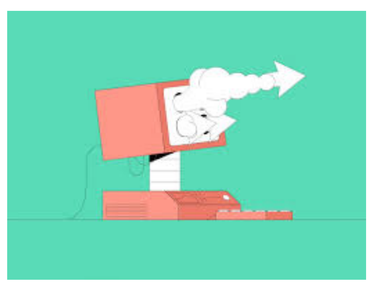
The Wired Guide to Cyberwar by Andy Greenburg, 23 September 2019. Available at https://www.wired.com/story/cyberwar-guide/ (Greenburg, 2019)

"Writing the Rules of Cyberwar" by Alyza Sebenius in The Atlantic. 28 June 2017. Available at https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/ (Sebenius, 2017)

Our Adversaries are Using Cyberwarfare. We Must Be Prepared by James Di Pane and Alexandra Marotta. 29 July 2019. Available at https://www.heritage.org/cybersecurity/commentary/our-adversaries-are-using-cyberwarfare-we-must-be-prepared (Di Pane & Marotta, 2019)

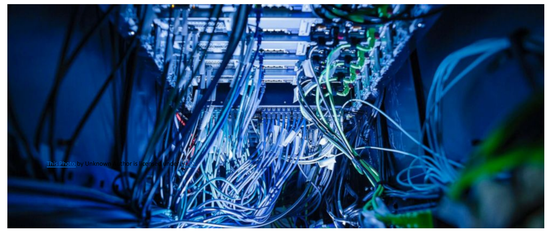
Waging (cyber)war in Peacetime by Fergus Hanson. 22 October 2015. Available at https://www.brookings.edu/blog/up-front/2015/10/22/waging-cyberwar-in-peacetime/ (Hanson, 2015)





Multimedia Resources

"Governments Don't Understand Cyberwarfare. We Need Hackers." Available at https://www.ted.com/talks/rodrigo_bijou_governments_don_t_understand_cyber_warfare_we_need_hackers.



This Photo by Unknown Author is licensed under CC BY-SA

This Photo by Unknown Author is licensed under CC BY-SA

Classroom Discussions, Debate Topics, or Essays

How does cyber warfare differ from traditional warfare, if at all?

Is international interference in national elections an act of war? Why or why not?

Does the historical formation and growth of the Internet lead to current cyberwarfare concerns? How or how not?

Is cyberspace militarized? If so, what do you think the biggest threat is? If not, should societies work to prevent it from becoming militarized?

What actions to prevent cyber warfare have different governments promoted?

References

Bijou, R. (2015, June). *Governments don't understand cyber warfare. We need hackers.* Retrieved from ted.com: https://www.ted.com/talks/rodrigo_bijou_governments_don_t_understand_cyber_warfare_we_need_hackers

Di Pane, J., & Marotta, A. (2019, July 29). *Our Adversaries Are Using Cyberwarfare. We Must Be Prepared.* Retrieved from heritage.org: https://www.heritage.org/cybersecurity/commentary/our-adversaries-are-using-cyberwarfare-we-must-be-prepared

Gazula, M. B. (2017). *Cyber Warfare Conflict Analysis and Case Studies.* MIT Management Sloan School, (IC)3. Cambridge, MA: Massachusetts Institute of Technology. Retrieved 7 24, 2020, from http://web.mit.edu/smadnick/www/wp/2017-10.pdf

Giles, K., & Hartmann, K. (2015). *Cyber Defense: An International View.* Carlisle Barracks, PA: United States Army War College Press. Retrieved from https://apps.dtic.mil/dtic/tr/fulltext/u2/a622264.pdf

Greenburg, A. (2019, 8 23). *The WiRED Guide to Cyberwar.* Retrieved from wired.com: https://www.wired.com/story/cyberwar-guide/

Hanson, F. (2015, October 22). *Waging (cyber)war in peacetime.* Retrieved from brookings.edu: https://www.brookings.edu/blog/up-front/2015/10/22/waging-cyberwar-in-peacetime/

Mazarr, M. J., Bauer, R. M., Casey, A., Heintz, S. A., & Matthews, L. J. (2019). *The Emerging Risk of Virtual Societal Warfare; Social Manipulation in a Changing Information Environment.* Santa Monica, CA: Rand. Retrieved from https://www.rand.org/pubs/research_reports/RR2714.html

Oxford University. (2020, 7 24). *interdisciplinary.* Retrieved from lexico.com: https://www.lexico.com/en/definition/interdisciplinary

Rand. (2020, 7 24). *Cyber Warfare.* Retrieved from rand.org: https://www.rand.org/topics/cyber-warfare.html#:~:text=Cyber%20warfare%20involves%20the%20actions,denial%2Dof%2Dservice%20attacks.

Schaeffer, D. M., Olson, P. C., & Knott Eck, C. (2017). An Interdisciplinary Approach to Cybersecurity Curriculum. *Journal of Higher Education Theory and Practice, 17*(9), 36-40.

Sebenius, A. (2017, June 28). *Writing the Rules of Cyberwar.* Retrieved from theatlantic.com: https://www.theatlantic.com/international/archive/2017/06/cyberattack-russia-ukraine-hack/531957/

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* Oxford: Oxford University Press.

The End!