Lesson Plan: An Interdisciplinary Approach to Teaching Cyber Warfare Concepts

Donna M. Schaeffer[1] and Patrick C. Olson[2]
[1]Marymount University, Arlington VA USA
[2]National University, San Diego, CA USA
Donna.schaeffer@marymount.edu
polson@nu.edu

Abstract: Interdisciplinary topics and fields need special attention to ensure that the breadth of the knowledge they represent are completely expressed. This is especially important and difficult to achieve in curriculum areas that tend to add new ideas on a constant basis and are sometimes interdisciplinary themselves. The topic/field cyber warfare is area this paper considers. This paper recommends and describes a lesson plan that provides the means of achieving a fully expressed examination of cyber warfare. The outcome is an articulation of the concept that will diffuse knowledge about cyber warfare. The lesson plan will be useful to any institution (particularly universities and government agencies) that need to diffuse knowledge about cyber warfare.

Keywords: Cyber Warfare; Curriculum Development

1. Introduction

Cyber warfare is an issue that has garnered attention, both in the media and in academia. For example, a news search for "cyber warfare" on the search engine Google yielded almost 300,000 hits in September 2022. The hits ranged from book reviews on the topic, articles from professional publications such as *Chief Privacy Officer* and *Modern Diplomacy,* and news sites such as Reuters. The movie franchise "Die Hard' Comes up in a Google search for "movies about cyber warfare." Undoubtedly, the term cyber warfare has entered popular parlance.

In the academic world, a search for "cyber warfare" on scholar.google.com in September 2022 identified over 100,000 items found. The sources ranged from books to well-regarded peer reviewed journals and conference proceedings from a wide variety of disciplines including computing and engineering, diplomacy and international relations, military sciences, and law.

If we accept the definition of interdisciplinary as relating to more than one branch of knowledge (Oxford University, 2020), the justification of cybersecurity as an interdisciplinary field (Schaeffer, Olson, & Knott Eck, 2017; Singer & Friedman, 2014) may be extended to cyber warfare.

In this paper, we present a lesson plan for introducing cyber warfare concepts to a variety of disciplines and using various pedagogies. The following sections of the paper identify competencies, describe learning objectives, discuss the need for varied resources, recommend appropriate reading and multi-media resources, describe classroom activities, and provide deliverables and assessment tools. We conclude with a general discussion of introducing the concepts of cyber warfare in an interdisciplinary fashion at various levels of study.

Singer and Freidman (2014) define cyber warfare as the use of technology to attack a nation, causing harm that is comparable to the harm sustained in actual warfare. In recent years, the definition has morphed into "actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through such as activities as computer viruses or denial-of-service attacks (Rand, 2020)." Gazula (2017) asserts "To many, cyber-warfare represents the 5th battle-space—a new type of warfare in need of further definition. To others, it is merely a new weapon to be integrated into traditional conflict."

The discourse on cyber warfare varies among disciplines, from a focus on nation-states in political science and international relations, terrorism in criminal justice studies, to protect and defend in computing. Table 1 displays excerpts from course descriptions in several disciplines. These course descriptions provide an overview of course-level inclusion of cyber warfare in programs. We have used these and other course descriptions to distill important concepts for one learning module about cyber warfare within a related course e.g., cybersecurity, criminal justice, and international relations.

Table 1: Excerpts from Cyberwarfare Course Descriptions

Excerpt	Institution	Discipline	Date
This course provides an overview of cyber warfare and the potential impact of its use by military, terrorist, and criminal organizations. An overview of cyber weaponry will be presented, and various offensive and defensive strategies will be examined via case studies.	American Public Universities	International Relations	nd
This course examines legal and policy challenges stemming from rapidly evolving cybersecurity threats. The course will begin with an introduction to cyber security and cyber warfare, and then explore the national and international legal frameworks that govern the cyberspace, including laws related to cybercrime, cyberespionage, and cyberwar.	Rutgers University	Law	nd
Provides an introduction to counterintelligence, with a focus on the evolution of contemporary counterintelligence in military, government, and pseudo-government organizations, both domestically and internationally. The course will also address terrorism as a criminally violent tactic used to achieve political or social goals and will examine individuals and groups, their motives and tactics, and how government and law enforcement have responded through investigation, prosecution, and punishment.	Marymount University	Criminal Justice	2020
This course examines traditional theories, concepts, and practices in international relations and warfare- conventional, unconventional, and modern- and relates them to the emerging dynamics of cyber war . . . The principal objective of this course is to introduce students to cyber war within the context of traditional, and emerging, concepts of armed and unarmed warfare.	Carnegie Mellon University	Political Science	2020
This course explores cyber warfare from an electrical engineering perspective. Rudimentary denial-of service techniques through intelligent wave form specific forms of computer network attack (CNA) are covered.	Naval Postgraduate School	Electrical Engineering	nd

2. Competencies

Learning competencies are skills students should acquire in a lesson, course, or degree program. Competencies may be identified by professional associations, disciplinary agreement, accrediting bodies, or by individual instructors. As cyber warfare is a relatively new academic topic, competencies from existing courses may introduce ideas for developing basic competencies we could expect learners to achieve from one lesson plan on cyberwarfare that is embedded within a wide range of disciplinary courses. Our suggestions are shown in Table 2.

Table 2: Suggested Competencies

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

3. Reading Materials.

To prepare lecture materials, instructors should read the 65-page tome from the Army War College entitled *Cyber Defense: An International Review* (Giles & Hartmann, 2015). This book provides a survey of approaches by the German, Swedish, Norwegian, and Estonian defense organizations. They should also read *The Emerging Risk of Virtual Societal Warfare* (Mazarr, Bauer, Casey, Heintz, & Matthews, 2019), a recent report from Rand Corporation.

College-level reading for students involves not only being able to read the text, but also to draw conclusions from it. Comprehension is a skill that students can develop. A course module on a sensitive topic, such as cyber warfare, requires student to read critically. Recommended readings for students in preparation for the lesson include short articles and book excerpts from media and think tanks across the political spectrum. Suggestions include (current URLs for each resource are provided in the references):

- The Wired Guide to Cyberwar by Andy Greenburg, 23 September 2019.
- "Writing the Rules of Cyberwar" by Alyza Sebenius in The Atlantic. 28 June 2017.
- Our Adversaries are Using Cyberwarfare. We Must Be Prepared by James Di Pane and Alexandra Marotta. 29 July 2019.
- Waging (cyber)war in Peacetime by Fergus Hanson. 22 October 2015.

4. Multimedia Resources.

Multimedia resources that could be employed either in a "flipped classroom" approach where students watch the video or listen to the audio before a class session or shown as an introduction to a class period. We recommend a brief 10-minute TedTalk by Rodrigo Bijou called "Governments Don't Understand Cyberwarfare. We Need Hackers." A current URL is provided in the References.

Several media outlets have posted recent short videos on cyberwarfare, including business outlets such as *Forbes* and *Fortune,* political outlets including C-Span and *Politico*, and general interest publications such as *National Geographic*. A professor needs to search videos on a search engine and select one from a trusted source or several that represent different orientations. Selection, and subsequent class activities, should be grounded in the cognitive theory of multimedia learning (Mayer and Moreno, 2003). This theory advances that students use multiple channels, that is visual and auditory, to make sense of new information. Figure 1 represents how information moves from a resource to students' knowledge base.

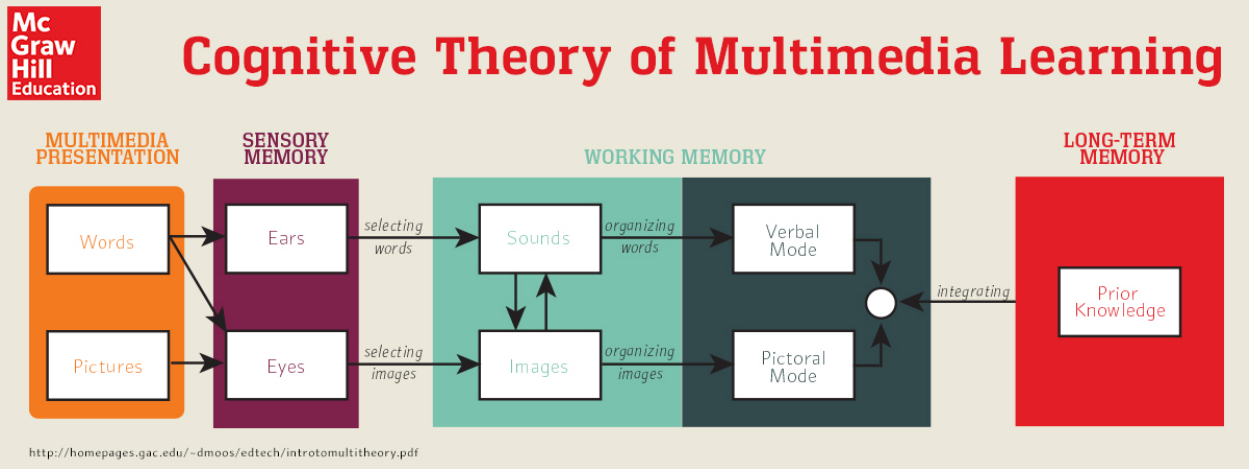

Figure 1: Cognitive Theory of Multimedia Learning (Source: https://www.mheducation.ca/blog/richard-mayers-cognitive-theory-of-multimedia-learning)

The Cognitive Theory of Multimedia Learning (CTML) recognizes that humans have a limited capacity for information. That is why we suggest presenting the same information in multiple ways to reinforce a limited number of cyberwarfare concepts, rather than a broad scope. It is also a rationale for selecting short videos.

5. Classroom Activities.

The CTML suggests learners actively engage with the material in order to learn it (McGrawHill Canada, 2019). After a brief lecture based on the suggested reading materials for instructors, there are several interactive activities that could be completed in the classroom or via online means in learning management systems. Activities should be designed around having students model cause-and-effects, make comparisons, apply generalizations, create enumerations, or develop classifications (Mayer and Moreno, 2003). We suggest activities and topics in the following section of this paper.

Reflection paper assignments enable students to think about how the learning experience changed them and the insights they have gained. Yancy (1998) describes reflection as needing both review of what has been learned and a projection of the student may use the information in the future.

Author F. Scott Fitzgerald is attributed with saying "The test of a first-rate intelligence is the ability to hold two opposed ideas in mind at the same time and still retain the ability to function." This describes debate assignments. Debates force students to see more than one side of an issue. Since cyberwarfare is a sensitive topic, and one on which students may come into the classroom with pre-conceived ideas, debates could add value. Debates also help build communication, collaboration, and critical thinking skills.

Role-playing is a pedagogical technique that is appropriate for complex concepts (Sogunro, 2004). Westrup and Planander (2013) found that role-playing increases both knowledge retention and student engagement. It helps student practice empathy and seeing issues from various perspectives (Elmore, n.d.).

Table 3 provides sample assignment topics that may be appropriate for the pedagogies discussed in the paper.

Table 3: Pedagogies and Appropriate Assignment Topics

Reflection Paper	Does cyber warfare differ from traditional warfare? If yes, how? If not, why not? (Sciarrone, 2017)
Debate	Statement: International interference in national elections is an act of war.
Role-playing	A group of government leaders have met to discuss what actions may be taken to prevent cyber warfare.

6. Conclusion.

This paper began by noting that cybersecurity and therefore cyber warfare is interdisciplinary and thus entire courses on cyber warfare are taught at various levels of study and in different disciplines are taught. To support the cyber warfare topic a lesson plan for a brief class section on cyber warfare that can be adapted to all levels of study, as well as tailored to specific disciplines was presented. The discussion included excerpts from courses, identification of competencies, recommended reading material and classroom activities.

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

Elmore, L.B. (n.d.) *Role-playing.* Retrieved from https://ablconnect.harvard.edu/role-play-research

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/

Mayer, R. E., & Moreno, R. (2003). Nine ways to reduce cognitive load in multimedia learning. *Educational psychologist*, *38*(1), 43-52.

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

McGrawHill Canada (2019, 16 April). *Richard Mayer's Cognitive Theory of Multimedia Learning.* Retrieved from McGrawHill Canada: https://www.mheducation.ca/blog/richard-mayers-cognitive-theory-of-multimedia-learning

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.

Sciarrone, M. (2017). Cyber Warfare: The New Front. *The Catalyst.* Issue 6. Retrieved from the George W. Bush Institute https://www.bushcenter.org/catalyst/modern-military/sciarrone-cyber-warfware.html#:~:text=Cyber%20warfare%20could%20make%20conventional,little%20use%20in%20the%20future.

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.

Sogunro, O.A. (2004). Efficacy of role-playing pedagogy in training leaders: Some reflections. *Journal of Management Development*, 23(4), 355-371

Yancy, K.B. (1998). *Reflection in the Writing Classroom.* Retrieved from Utah State University: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1119&context=usupress_pubs&_ga=2.227644339.927502929.1663441304-1372834558.1663441304

Westrup, U. & Planander, A. (2013). Role-play as a pedagogical method to prepare students for practice: The students' voice. Ogre utbildning, 3(3), 199-210.