"When warranted the US will respond to hostile acts in cyberspace as we would to any other threat to our country."

President Barack Obama
The International Strategy For Cyberspace, May 2011

1. Introduction
This elective seeks to balance the theoretical and the technical. The goal is placing cyber warfare in the context of military history. What is its place in the evolution of states at war? The technical is not ignored, however. How these attacks have evolved technologically is a key point of analysis. Case studies become fundamental to such a course to not only better illustrate the themes addressed above, but to emphasize new realities on the traditional battlefield. They include China and its efforts to steal US data, the Israeli effort—with US assistance or consent—to curb Iran’s nuclear program, and conflict applications such as the Russian attack on Georgia. Moreover, that cyber warfare can threaten (and enhance) not just military capabilities, but financial institutions and private industry, as well as national infrastructure, expands the nature of cyber warfare. In this light, informational warfare falls within the cyber war purview as well since the technology, and its application, impacts social-cultural realities, perhaps transforms them into world changing events that spark future security challenges. In short, an examination of cyber warfare requires a close look at the long tradition of a “western” way of war.

2. Student Learning Outcomes
   1.1 Analyze classical and emerging theories of the enduring nature and changing character of war.
   1.2 Analyze the nature and character of war as interrelated military, political, economic, and social activities.
      2.1 Comprehend the concept and facets of national power.
      2.2 Comprehend stakeholder functions in national security decision-making.
      2.3 Comprehend the global security environment and U.S. strategy and policy within their historical context.
      2.4 Analyze joint and Marine Corps doctrine and emerging concepts, and their application within joint and multinational operations.
      3.4 Apply appropriate modes of cross-cultural interaction to planning, programming, and operations.
      3.5 Analyze the dynamic interaction between cultures in conflict across the Range of Military Operations.
      4.1 Recognize the complexity and nature of problems.
      4.4 Analyze cognitive processes that affect decision making.
      4.5 Apply insights from history and other academic disciplines to enhance decision making.
      5.3 Analyze the factors involved in leading and implementing transitions.
6.5 Evaluate different organizational cultures and their effects on performance and ethical behavior.

7.4 Recognize the opportunities and vulnerabilities created by widespread information dissemination enabled by emerging media.

3. Supporting Educational Objectives
   a. Demonstrate the ability to assess the role of cyber technology at each level of war and ensure necessary integration during planning and execution for strategic success. (JPME 1f, 3b, 3c, 4d, 4g, 5c, 6b, 6c)
   b. Demonstrate knowledge of Cyber strategies, concepts and emerging technologies that support the planning and execution of joint and multinational operations. (JPME 1f, 2e, 4a, 4c, 4d, 4f, 4g, 5c)
   c. Demonstrate the ability to apply lessons learned from history to the planning and execution of military operations. (JPME 4d)

4. Student Requirements

Seminar 1, Monday, 26 January 2015
Defining Cyber Warfare
Covers recent cyber events to ask if these cyber “attacks” constitute something new in terms of warfare/conflict.

(1) Location: Command and Staff College, RM 214
(2) Instructor: M. Flynn
(3) Required Reading (66 pages):
      -John Stone, “Cyber War Will Take Place.”
      -Gary McGraw, “Cyber War is Inevitable (Unless We Build in Security).”
      -Timothy J. Junio, “How Probable is Cyber War?: Bringing IR Theory Back in to the Cyber Conflict Debate.”
      -Adam P. Liff, “The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio.”
(4) Supplemental Reading
Marine Corps University / Command and Staff College  
The Electives Program

http://online.wsj.com/article/SB10001424052748704671904575193942114368842.html
e. Review of Richard Clarke’s *Cyber War*, Jerry Brito and Tate Watkins, “Wired Opinion: Cyberwar is the New Yellow Cake,” *Wired*, 14 February 2012. (2)  
http://www.wired.com/threatlevel/2012/02/yellowcake-and-cyberwar/
http://smallwarsjournal.com/jrnl/art/the-case-for-cyber

(5) Issues for Consideration:
   a. What is cyber?
   b. Does cyber technology represent a revolution in military affairs?
   c. Is there value to the warfighter recognizing that when utilizing cyber technology, they are operating in a “new” context?

Seminar 2, Thursday, 29 January 2015
*US Policy in Cyberspace*
Covers US military strategy in cyberspace in the context of Clausewitz and Sun Tzu.

(1) Location: Command and Staff College, RM 214
(2) Instructor: Michael Warner, US Cyber Command historian
(3) Required Reading (78 pages):
Marine Corps University / Command and Staff College

The Electives Program

(September 2009), 1-6. (6 pages)
http://www.ndu.edu/CTNSP/docUploaded/DH68.pdf


(4) Supplemental Reading

g. Ryan Singel, “Congress Authorizes Pentagon to Wage Internet War,” Wired, 14 Dec 2011 (1)

(5) Issues for Consideration:

a. What is US cyber policy?
b. What physical systems are available to the warfighter at the strategic, operational, and tactical levels of war?
c. Define defensive, offensive and exploitation in cyber operations.

Seminar 3, Monday, 2 February 2015

China and Information Theft

Covers the difficulty of defining acts of war in cyberspace specifically looking at intellectual property theft and the supposed foremost offender.

(1) Location: Command and Staff College, RM 214
(2) Instructor: Prof Flynn
(3) Required Reading (77 pages):


(4) Supplemental Reading


b. Mandiant, “APT 1, Exposing One of China’s Cyber Espionage Units,” February 2013. (76)

c. Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*.


http://search.proquest.com.lomc.idm.oclc.org/docview/223083647/fulltext/13B7BEDAB4257C69805/1?accountid=14746


http://www.uscc.gov/Research/occupying-information-high-ground-chinese-capabilities-computer-network-operations-and

i. Dan Blumenthal, “How to Win a War Against China,” *Foreign Policy Magazine*, 28 February 2013. (2)

(5) Issues for Consideration:

a. What constitutes a cyber attack?

b. Is the United States in a “cyber war” with China?
c. Does Chinese theft of data constitute an act of war?
d. How does one assign attribution in a cyber environment?

Seminar 4, Thursday, 5 February 2015

Russia and Cyber Warfare
Covers Russia’s use of cyber attacks in its wars against Estonia and Georgia.
(1) Location: Command and Staff College, RM TBD
(2) Instructor: Dave Hollis, Chief, J51 Strategy Div. USCYBERCOM
(3) Required Reading (80 pages):
      http://www.carlisle.army.mil/USAWC/parameters/Articles/08winter/korns.pdf

(4) Supplemental Reading

(5) Issues for Consideration:
   a. How successful was the Russian cyber attack on Georgia?
   b. Did the Russians successfully mix kinetic and non-kinetic components in their attack?
   c. Did the Russian strike represent a “new” type of attack, or continue to exemplify a western way of war?

Seminar 5, Monday, 9 February 2015

Cyber and International Law
Examines the application of international law and cyber conflict.
(1) Location: Command and Staff College, RM 214
(2) Instructor: Kurt Sanger, MARFORCYBER
(3) Required Reading (78 pages):
      http://www.usnwc.edu/getattachment/8da8759f-6a32-419d-b813-e7f4f1ec5a62/Waxman.aspx
Marine Corps University / Command and Staff College
The Electives Program


(4) Supplemental Reading:

a. “No Legal Vacuum in Cyber Space,” International Committee of the Red Cross, *Resource Centre* (2)

b. Stewart Baker, “What is the Role of Lawyers in Cyberwarfare?” *ABAJournal*, May 1, 2012 (4)
   http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/

   Assigned reading: pages 42-95 (53)
   http://www.cccdcoe.org/249.html


(5) Issues for Consideration:

a. What are the legal parameters of war in cyberspace?

b. Are laws governing cyber warfare too “western” centric?

c. How different are the laws governing cyber warfare than past laws governing warfare?

Seminar 6, Wednesday, 11 February 2015

**Stuxnet: Guerrilla Warfare in Cyberspace**

Covers the issue of attribution regarding the actions of state actors and hackers and non-state actors when it comes to releasing viruses and other malware.

(1) Location: Command and Staff College, RM 214

(2) Instructor: M. FLYNN

(3) Required Reading (73 pages):


(4) Supplemental Reading
b. “Hacktivism: Cyberspace has Become the New Medium for Political Voices,” White Paper, McAfee, May 2012. (18)  
   http://vrritti.com/2012/07/05/mcafee-report-hacktivism-cyberspace-has-become-the-new-medium-for-political-voices/

(5) Issues for Consideration:
   a. Does a virus represent a cyber attack?
   b. Was the Stuxnet attack successful?
   c. How vulnerable is Iran’s nuclear program to cyber attack?

Seminar 7, Tuesday, 17 February 2015
The Cyber-led Revolution
Covers the Arab Spring and the role of social media and networking.
   (1) Location: Command and Staff College, RM 214
   (2) Instructor: Dr. Flynn
   (3) Required Reading (77 pages):

(4) Supplemental Reading:
b. David C. Benon, “Why the Internet Is Not Increasing Terrorism,” 


(5) Issues for Consideration:
   a. Did social networking cause the Arab Spring?
   b. Has the Arab Spring been a positive or negative event?
   c. What is the future of the Middle East given the Arab Spring? What about other parts of the world?

Seminar 8, Thursday, 19 February 2015
A New Cold War: Deterrence in Cyberspace
Addresses the likelihood of confining conflict to the cyber domain.
(1) Location: Command and Staff College, RM 214
(2) Instructor: M. Flynn
(3) Required Reading (78 pages):

(4) Supplemental Reading

(5) Issues for Consideration:
   a. What should deterrence look like in cyberspace? Is it possible or desirable?
   b. Is the Cold War a model for cyber deterrence?
   c. Does cyber deterrence reinforce or detract from international cyber norms?
Seminar 9, Monday, 23 February 2015

*Cyber as Economic Warfare*

Covers cyber ties to marshaling state resources including extending government protection to critical infrastructure.

(1) Location: MCIA
(2) Instructor: Director, INTERPOL DC
(3) Required Reading (69 pages):

(4) Supplemental Reading:

(5) Issues for Consideration:
   a. Is cyber warfare economic warfare?
   b. What role should the US military play in defending the homeland’s infrastructure?

Seminar 10, Thursday, 26 February 2015

*The New Militia: The Warfighter in the Cyber Domain*

Addresses what role civilians should play in a cyber war.

(1) Location: Command and Staff College, RM TBD
(2) Instructor: Prof Flynn
(3) Required Reading (73 pages):
Marine Corps University / Command and Staff College
The Electives Program


(4) Supplemental Reading


(5) Issues for Consideration:

a. How has the private sector directed and defined cyber war?

b. How does the civil-military relationship work with cyber defense issues?

c. What are the assigned roles of US defense organizations in cyber defense?

5. Evaluations

Students must read the assigned readings, contribute to scheduled seminars, develop a cyber plan, conduct an exercise executing that plan, write an information paper, and write an essay paper.

a. Seminar Participation (40%). Each student will be required to contribute to the discussions during each seminar. Emphasis will be placed on quality of participation over quantity of participation.

b. Course Paper (40%). Each student will present a “review” of one aspect of cyber warfare. The course paper is due at the beginning of the final seminar and should be 5 pages. Your paper should be double-spaced, with one inch margins, prepared in 12 point pitch, Times New Roman font, with endnotes and a bibliography.

c. Seminar Presentation (20%). The students will present in seminar their findings of the “cyber capabilities” of a nation-state. The presentation consists of a five-minute talk in which the student presents their analysis and conducts a 5-minute Q&A session. The report is formally submitted in writing to the professor as well.

6. Relationship to Other Instruction
This elective relates to eight of the nine published Warfighting Learning Objectives as well as thirteen of the Joint Learning Objectives. This elective takes the basic cyber instruction provided to all of the students and provides the appropriate venue to explore each topic further.

7. References
There is a host of additional reading available. CSC, MCU is working on a recommended reading list that will be accessible online.

Lesson Hours:

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Guest Lecture</th>
<th>Seminar discussion</th>
<th>Film</th>
<th>Practical Application</th>
<th>Staff Ride/ Battle study</th>
<th>Evaluation/Test</th>
<th>Student Preparation Time</th>
<th>TOTAL HOURS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>40</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>60</td>
</tr>
</tbody>
</table>

JPME Data (JPME level):

<table>
<thead>
<tr>
<th>Area 1</th>
<th>Area 2</th>
<th>Area 3</th>
<th>Area 4</th>
<th>Area 5</th>
<th>Area 6</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>b</td>
<td>C</td>
<td>d</td>
<td>e</td>
<td>F</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
</tr>
<tr>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
<td>e</td>
<td>f</td>
</tr>
</tbody>
</table>

IAW CJCSI 1800.01D