

**Marine Corps University / Command and Staff College**  
*The Electives Program*

**Course Title: Cyberspace and the  
Intellectual Revolution**

**Date: 26 Jan 15 – 26 Feb 15, 0900-1100**  
**Author: Prof Flynn**

*"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.

**Marine Corps University / Command and Staff College**  
*The Electives Program*

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):

a. Matthew J. Flynn, “Is There a Cyber War? Review Essay,” *National Cyber Security Institute Journal*, Vol. 1, No. 2 (2014): 5-8. (3 pages)  
<http://ncij.excelsior.edu/article/is-there-a-cyber-war/>

b. “Cyber Roundtable,” *Journal of Strategic Studies*, Vol. 36, Issue 1 (2013): 101-142. (31 pages)

-John Stone, “Cyber War Will Take Place.”

-Gary McGraw, “Cyber War is Inevitable (Unless We Build in Security).”

-Dale Peterson, “Offensive Cyber Weapons: Construction, Development, and Employment.”

-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.”

-Thomas Rid, “More Attacks, Less Violence.”

c. Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth.” *International Security*, Vol. 38, No. 2 (Fall 2013): 41-73. (32 pages)

(4) Supplemental Reading

a. James A. Lewis, “Conflict and Negotiation in Cyberspace,” Center for Strategic and International Studies (CSIS), February 2013. Pp. 70.

b. Martin C. Libicki, “Cyberdeterrence and Cyberwar,” RAND Corp, Prepared for the Air Force, 2009. Pp. 240.

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- c. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins Publishers, 2010). Pp. 290.
  - d. Book Review of Richard Clarke's *Cyber War*, *Wall Street Journal*, April 2010. (2)  
<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/>
  - f. Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013). Pp. 207.
  - g. John Brickey, "The Case for Cyber," *Small Wars Journal*, Sept 13, 2012. (9)  
<http://smallwarsjournal.com/jrnl/art/the-case-for-cyber>
  - h. LTC Scott Stephenson, "The Revolution in Military Affairs: 12 Observations on an Out-of-Date Idea," *Military Review* (May-June 2010): 38-46. (9)  
<http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=3666456&site=ehost-live>
- (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):
  - a. David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *The Journal of Strategic Studies*, Vol. 35, No. 5 (Oct 2012): 689-711. (22 pages)
  - b. Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol. 38, No. 2 (Fall 2013): 7-40. (33 pages)
  - c. Ross M. Rustici, "Cyberweapons: Leveling the International Playing Field," *Parameters* (Autumn 2011): 32-42. (11 pages)  
<http://lomc.idm.oclc.org/login?url=http://search.proquest.com/docview/928971315?accountid=14746>
  - d. Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21<sup>st</sup>-century War," *Defense Horizons*, Number 68

**Marine Corps University / Command and Staff College**  
*The Electives Program*

(September 2009), 1-6. (6 pages)

<http://www.ndu.edu/CTNSP/docUploaded/DH68.pdf>

- e. Robert A. Miller, Daniel T. Kuehl, and Irving Lachow, "Cyber War: Issue in Attack and Defense." *Joint Force Quarterly*, Issue 61, 2<sup>nd</sup> Quarter 2011: 18-23. (6 pages)

(4) Supplemental Reading

- a. Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game," *Strategic Studies Quarterly* (Winter 2012): 100-118. (18)
- b. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *The Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012): 401-428. (27)
- c. Colin S. Gray, "Making Strategic Sense of Cyber Power: Why the Sky is not Falling," (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2013). Pp. 67.
- d. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future Strategy and History*, eds. Colin Gray and Williamson Murray (London: Frank Cass, 2004). Pp. 263.
- e. Derek S. Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press, 2012). Pp. 246.
- f. Gen. Huba Wass de Czege, US Army Rtr., "Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack," *Military Review* (July-August 2010): 85-96. (12)  
<http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=53153881&site=ehost-live>
- g. Ryan Singel, "Congress Authorizes Pentagon to Wage Internet War," *Wired*, 14 Dec 2011 (1)  
<http://www.wired.com/threatlevel/2011/12/internet-war-2/>

(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):

- a. Nina Hachigian, "China's Cyber-Strategy," *Foreign Affairs* (March-April 2001), 118-133. (17 pages)

<http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=4127141&site=ehost-live>

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- b. Timothy L. Thomas, "Google Confronts China's 'Three Warfares'," *Parameters* (Summer 2010): 101-113. (13 pages)  
<http://www.carlisle.army.mil/USAWC/parameters/Articles/2010summer/Thomas.pdf>
  - c. Gurmeet Kanwal, "China's Emerging Cyber War Doctrine," *Journal of Defence Studies*, Vol. 3, No. 3 (July 2009): 14-22. (8 pages)
  - d. Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 4, No. 2 (2011): 1-24. (24 pages)
  - e. Johan Lagerkvist, "New Media Entrepreneurs in China: Allies of the Party-State or Civil Society?" *Journal of International Affairs* Vol. 65, No. 1 (Fall/Winter 2011): 169-182. (13 pages)
- (4) Supplemental Reading
- a. Li Zhang, "A Chinese Perspective on Cyber War," *International Review of the Red Cross*, Vol. 94, No. 886 (Summer 2012): 801-807. (6)  
<http://www.icrc.org/eng/assets/files/review/2012/irrc-886-zhang.pdf>
  - b. Mandiant, "APT 1, Exposing One of China's Cyber Espionage Units," February 2013. (76)  
[http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf)
  - c. Qiao Liang and Wang Xiangsui. *Unrestricted Warfare*.
  - d. Tim Thomas, *Decoding the Virtual Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2007). Pp. 352.
  - e. ----- . *Dragon Bytes: Chinese Information-war Theory and Practice from 1995-2003* (Fort Leavenworth, KS: Foreign Military Studies Office, 2004). Pp. 168.
  - f. James Fallows, "Cyber Warriors," *The Atlantic Magazine*, March 2010. (5)  
<http://search.proquest.com/lomc.idm.oclc.org/docview/223083647/fulltext/13B7BEDAB4257C69805/1?accountid=14746>
  - g. Lolita C. Baldor and Robert Burns, "Pentagon Discloses Massive Cyber Theft," *Associated Press*, July 2011. (1)  
[http://www.msnbc.msn.com/id/43757768/ns/technology\\_and\\_science-security/t/pentagon-discloses-massive-cyber-theft/from/toolbar](http://www.msnbc.msn.com/id/43757768/ns/technology_and_science-security/t/pentagon-discloses-massive-cyber-theft/from/toolbar)
  - h. Bryan Krekel, Patton Adams, George Bakos, "Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Northrop Grumman Corp, Prepared for the US-China Economic and Security Review Commission, 7 March 2012. (137)  
<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?

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- 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):
  - a. CPT Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* (November-December 2011): 63-68. (7 pages)  
<http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=67643241&site=ehost-live>
  - b. Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-2009): 60-76. (17 pages)  
<http://www.carlisle.army.mil/USAWC/parameters/Articles/08winter/korns.pdf>
  - c. David M. Hollis, "Cyber War Case Study, Georgia 2008," *Small Wars Journal*, January 6, 2011. (10 pages)  
<http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>
  - d. "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence (CCDCOE), Tallinn, Estonia, November 2008. (46 pages)
- (4) Supplemental Reading
  - a. Asmus, Ronald D. *A Little War That Shook the World: Georgia, Russia, and the Future of the West*. New York: Palgrave Macmillan, 2010. Pp. 272.
- (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):
  - a. Matthew C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies*, Vol. 89 (2013): 109-122 (15 pages)  
<http://www.usnwc.edu/getattachment/8da8759f-6a32-419d-b813-e7f4f1ec5a62/Waxman.aspx>

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- b. Rex Hughes, "A Treaty for Cyberspace." *International Affairs* 86: 2 (2010): 523-541. (18 pages)
  - c. Todd C. Huntley, "Controlling the Use of Force in Cyberspace: The Application of the Law of Armed Conflict During a Time of Fundamental Change in the Nature of Warfare," *Naval Law Review*, Vol. 60 (2010): 1-40. (40 pages)
  - d. Kyle Genaro Philips, "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain," *Joint Forces Quarterly*, Issue 70, 3<sup>rd</sup> Quarter 2013: 70-75. (5 pages)
- (4) Supplemental Reading:
- a. "No Legal Vacuum in Cyber Space," International Committee of the Red Cross, *Resource Centre* (2)  
<http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>
  - b. Stewart Baker, "What is the Role of Lawyers in Cyberwarfare?" *ABA Journal*, May 1, 2012 (4)  
[http://www.abajournal.com/magazine/article/what\\_is\\_the\\_role\\_of\\_lawyers\\_in\\_cyberwarfare/](http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/)
  - c. NATO, Cooperative Cyber Defense Centre of Excellence, *The Tallinn Manual*, Tallinn, Estonia (Cambridge University, 2013), pp. 265. Assigned reading: pages 42-95 (53)  
<http://www.ccdcoe.org/249.html>
  - d. Rex Hughes, "A Treaty for Cyberspace," *International Affairs* 86:2 (2010): 523-541. (18)
  - e. Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge: Cambridge University, 2012). Pp. 331.
- (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):

- a. Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (2013): 365-404. (39 pages)
- b. Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *JFQ*, Issue 63, 4<sup>th</sup> Quarter 2011: 70-73. (17 pages)  
<http://lomc.idm.oclc.org/login?url=http://search.proquest.com/docview/926433852?accountid=14746>

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- c. Paolo Shakarian, "Stuxnet: Cyberwar Revolution in Military Affairs," *Small Wars Journal*, 15 April 2011. (10 pages)
  - d. Lucas Milevski, "Stuxnet and Strategy: a Special Operation in Cyber Space?," *JFQ*, Issue 63, 4<sup>th</sup> Quarter 2011: 64-69. (6 pages)  
<http://www.ndu.edu/press/stuxnet-and-strategy.html>
- (4) Supplemental Reading
- a. Nicholas Falliere, "W32: Stuxnet Dossier," *Symantec Security Response*, Version 1.4 (February 2011): 1-69. BB
  - 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/>
  - c. Steven Metz, "The Internet, New Media, and the Evolution of Insurgency," *Parameters*, Vol. XLII, No. 3 (Autumn 2012): 80-90. (10)
- (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):
  - a. Mariam Esseghaier, "'Tweeting Out a Tyrant,' Social Media and the Tunisian Revolution," *Wi Journal of Mobile Media* Vol. 7, No. 1 (March 2013). (8 pages)  
<http://wi.mobilities.ca/tweeting-out-a-tyrant-social-media-and-the-tunisian-revolution/#>
  - b. Jon Alterman, "The Revolution will not be Tweeted," *The Washington Quarterly* 34(4) (2011): 103-116. (13 pages)
  - c. Judy Bachrach, "Wikihistory: Did the Leaks Inspire the Arab Spring?" *World Affairs* (July/Aug 2011): 35-44. (9 pages)
  - d. Victor D. Cha and Nicholas D. Anderson, "A North Korean Spring," *The Washington Quarterly* Vol. 35, No. 1 (2012): 7-24. (17 pages)
  - e. Dubai School of Government, "Civil Movements: The impact of Facebook and Twitter," *Arab Social Media Report*, 1(2) (May 2011): 1-30. (30 pages)  
<http://unpan1.un.org/intradoc/groups/public/documents/dsg/unpan044212>
- (4) Supplemental Reading:
  - a. United States Institute of Peace, "New Media and Conflict after the Arab Spring," *Peaceworks* 80 (2012): 1-24. (24)

**Marine Corps University / Command and Staff College**  
*The Electives Program*

- b. David C. Benon, "Why the Internet Is Not Increasing Terrorism," *Security Studies*, Vol. 23, No. 2 (2014): 293-328. (35)
  - c. "The Internet and Youth Subculture in Kuwait," In Deborah Wheeler, *The Internet in the Middle East: Global Expectations and Local Imaginations in Kuwait* (Albany, NY: SUNY Press, 2006): 133-162. (29)
  - d. Robert I Rotberg and Jenny C. Aker, "Mobile Phones: Uplifting Weak and Failed States," *The Washington Quarterly*, Vol. 36, No. 1 (2013): 111-125. (14)
  - e. Michael S. Doran, "The Impact of New Media: The Revolution Will be Tweeted," in Kevin Pollack, et al eds., *The Arab Awakening: America and the Transformation of the Middle East* (Washington D.C.: Brookings Institute Press): 39-46. (7)
- (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):
  - a. William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, Issue 5 (Sept-Oct 2010): 97-108. (11 pages)
  - b. Matthew D. Crosston, "World Gone Cyber MAD: How 'Mutually Assured Debilitation' Is the Best Hope for Cyber Deterrence," *Strategic Studies Quarterly* (Spring 2011): 100-116. (16 pages)
  - c. Will Goodman, "Cyber Deterrence: Tougher in Theory Than in Practice," *Strategic Studies Quarterly* (Fall 2010): 102-135. (33 pages)
  - d. Eric Sterner, "Retaliatory Deterrence in Cyberspace," *Strategic Studies Quarterly* (Spring 2011): 62-80. (18 pages)
- (4) Supplemental Reading
  - a. Tim Stevens, "A Cyber War of Ideas: Deterrence and Norms in Cyberspace," *Contemporary Security Policy*, Vol. 33, No. 1 (April 2012): 148-170. (22)
  - b. Joseph Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* (Winter 2011): 18-38. (20)
- (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?

**Marine Corps University / Command and Staff College**  
*The Electives Program*

**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):
  - a. *Cyber and Physical Security, Special Report*, “When Worlds Collide: The Converging Threats to Government’s Cyber and Physical Infrastructure,” A Research Report from the Center for Digital Government, 2012. (32 pages)
  - b. “In the Dark: Crucial Industries Confront Cyberattacks,” McAfee and CSIS, April 2011. (28 pages)  
<http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf>
  - c. Keith B. Alexander, Emily Goldman, Michael Warner, “Defending America in Cyberspace,” *The National Interest*, No 128 (Nov/Dec 2013): 18-24. (7 pages)
  - d. “Panetta Warns of Dire Threat of Cyberattack on US,” *The New York Times*, 11 Oct 2012. (2 pages)
- (4) Supplemental Reading:
  - a. “Linking Cybersecurity, Policy, and Performance,” Microsoft, 2013. (27)
  - b. “2010 Data Breach Investigations Report,” A Study Conducted by the Verizon RISK Team in Cooperation with the United States Secret Service, Verizon, 2010. (66)
  - c. “Defining the Threat, Forging a Strategy,” International Assessment and Strategy Center (IASC), Prepared for the Department of Homeland Security, 30 July 2012. (62)
  - d. Edward G. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Amsterdam: Elsevier, 2011).
  - e. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (New York: The Penguin Press, 2011).
- (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*

- a. Matthew Crosston, "Virtual Patriots and a New American Cyber Strategy: Changing the Zero-Sum Game," *Strategic Studies Quarterly* (Winter 2012): 100-118. (18 pages)
  - b. Gregory Conti, "Leadership of Cyber Warriors: Enduring Principles and New Directions," *Small Wars Journal*, July 11, 2011. (10 pages)  
<http://www.smallwarsjournal.com/blog/journal/docs.../811-contiraymond.pdf>
  - c. Gregory Conti, "Self-development for Cyber Warriors," *Small Wars Journal*, November 10, 2011. (34 pages)  
<http://www.smallwarsjournal.com/sites/default/files/893-conti.pdf>
  - d. Kamal Jabbour, "Cyber Vision and Cyber Force Development," *Strategic Studies Quarterly*, Spring 2010: 63-74. (11 pages)
- (4) Supplemental Reading
- a. Gregory Conti, "Recruiting, Development, and Retention of Cyber Warriors Despite an Inhospitable Culture," *Small Wars Journal*, July 29, 2010. (11)  
<http://www.smallwarsjournal.com/blog/journal/docs-temp/482-conti-easterly.pdf>
  - b. Stew Magnuson, "Do Cyber Warriors Belong at Special Operations Command," *National Defense*, July 2011. (1)  
<http://www.nationaldefensemagazine.org/archive/2011/August/Pages/DoCyberwarriorsBelongatSpecialOperationsCommand.aspx>
- (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**

**Marine Corps University / Command and Staff College**  
*The Electives Program*

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:**

Lecture	Guest Lecturer	Seminar discussion	Film	Practical Application	Staff Ride/ Battle study	Evaluation/Test	Student Preparation Time	TOTAL HOURS
		20					40	60

**JPME Data (JPME level):**

Area 1						Area 2					Area 3					Area 4							Area 5			Area 6			
a	b	C	d	e	F	a	b	c	d	e	a	b	c	d	e	f	a	b	c	d	e	f	g	a	b	c	a	b	c
					2					1		1	1				2			3		1	2			2		1	1

IAW CJCSI 1800.01D