

Marine Corps University / Command and Staff College
The Electives Program

Lesson Title: Cyberwarfare
(this syllabus is unclassified, but course sessions include TS material)

Date: 26 Jan – 26 Feb 16
Author: Prof Gary Brown
Revision Date: AY 15-16

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

International Strategy for
Cyberspace (May 2011)

1. Introduction

This course will focus on the use of cyber capabilities in warfare, preservation of national interests and espionage. It will provide technical, legal and policy background to provide context to the discussion. In addition to U.S. practice, the cyber activities of Russia, China and Iran will be a focus of the course, although other states will also be part of the conversation. The topics to be discussed include encryption, privacy, data mining and social networking, all within the context of military operations. The course will provide students the background and vocabulary to discuss the role of cyber capabilities at a high level, enabling them to help shape the future of cyberspace operations.

2. Student Learning Outcomes

- 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.
- 4.1 Recognize the complexity and nature of problems.
- 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.
- b. Demonstrate knowledge of Cyber strategies, concepts and emerging technologies that support the planning and execution of joint and multinational operations.
- c. Demonstrate the ability to apply lessons learned from history to the planning and execution of military operations.

4. Student Requirements

a. Class 1, 26 January 2016, *Cyber Basics & Some History*

Selected cyber events and some technical background to facilitate discussion throughout the rest of the course.

(1) Required Reading (70 pages):

(a) Dan Verton, "U.S. cyber policy struggles to keep up with events," *Fed Scoop* (27 July 2015). (2 pages) <http://fedscoop.com/u-s-cyber-policy-struggling-to-keep-up-with-events> **Online**

(b) P.W. Singer & Allan Friedman, "How It All Works," *Cybersecurity & Cyberwar* (2014). pp. 12-45, (33 pages) **Blackboard**

Marine Corps University / Command and Staff College
The Electives Program

(c) Jason Andress & Steve Winterfeld, "Logical Weapons," Cyber Warfare (2011), pp. 83-118. (35 pages) **Blackboard**

(2) Supplemental Reading:

(a) LTC Scott Stephenson, "The Revolution in Military Affairs: 12 Observations on an Out-of-Date Idea," *Military Review* (May-June 2010), pp. 38-46. (9 pages) http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview20100630_art007.pdf

(b) Michael Lewis, Flash Boys (2014), pp. 7-22, 56-82. (41 pages)

(3) Issues for Consideration:

(a) What is cyberspace?

(b) Does cyber technology represent a revolution in military affairs?

(c) What's the relevance of these two questions to the warfighter?

(d) In 1993, in *A History of Warfare* John Keegan said, "War is not the continuation of policy by other means [as that] implies the existence of states, of state interests and of rational calculation about how they may be achieved." Does the rise of cyber warfare since then make his statement more or less accurate?

b. Class 2, 29 January 2016, Terms of Debate & More Background

Additional information about the debates surrounding cyber operations and policy.

(1) Instructor: Jim Penrose

(2) Required Reading (63 pages):

(a) William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (Sept./Oct. 2010). (13 pages)
<https://www.foreignaffairs.com/articles/united-states/2010-09-01/defending-new-domain>

Online

(b) Excerpts from various cyber lexicons (10 pages) **Provided**

(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> **Online**

(d) John Stone, "Cyber War Will Take Place," *Journal of Strategic Studies*, Vol. 36, No. 1 (2013), pp. 101-108 (8 pages)

<http://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.730485> **Online**

(e) Singer & Friedman, pp. 45-66. (21 pages) **Blackboard**

(3) Supplemental Reading:

(a) David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *The Journal of Strategic Studies*, Vol. 35, No. 5 (Oct 2012), pp. 689-711. (22 pages)

<http://www.tandfonline.com/doi/pdf/10.1080/01402390.2012.706970>

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

(c) 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), pp. 401-428. (27 pages)

Marine Corps University / Command and Staff College
The Electives Program

(d) Gen. Huba Wass de Czege, US Army Rtr., “Warfare by Internet: the Logic of Strategic Deterrence, Defense, and Attack,” *Military Review* (July-August 2010), pp. 85-96. (12 pages)

<http://lomc.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=53153881&site=ehost-live>

(e) 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. 12-32. (20 pages)

(f) Thomas Rid, *Cyber War Will Not Take Place* (Oxford University Press, 2013).

(4) Issues for Consideration:

(a) Which definitions best facilitate understanding and operations in cyberspace?

(b) How can we best conceptualize the cyber domain to maximize understanding by military and political leaders?

(c) What’s the difference between cyber warfare and cyber crime? What are the implications of making the distinction?

c. Class 3, 2 February 2016, Threat & Response 1: China

The U.S. relationship with China from a cyberspace perspective, as well as the issues surrounding intellectual property theft.

(1) Instructor: LtCol Adam Jenkins

(2) Required Reading (43 pages):

(a) Nakashima, “Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies,” *Washington Post* (27 May 2013). (2 pages) https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html **Online**

(b) George Chen, Steve Dickinson, David Schlesinger, Xiao Qiang, Rogier Creemers & David Wertime, “China’s Great Firewall Is Rising,” *Foreign Policy* (3 Feb 2015). (10 pages) <http://foreignpolicy.com/2015/02/03/china-great-firewall-is-rising-censorship-internet/> **Online**

(c) Citizen Lab, *China’s Great Cannon* (10 Apr 2015), pp. 1-12. (12 pages) <https://citizenlab.org/2015/04/chinas-great-cannon/> **Online**

(d) Department of Justice Fact Sheet, “U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage” (19 May 2014). (1 page) <http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor> **Online**

(e) White House Fact Sheet, *President Xi Jinping’s State Visit to the United States* (25 Sept 2015), pp. 4-5. (2 pages) <https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states> **Online**

(f) Andrea Shalal, “Top U.S. spy says skeptical about U.S.-China cyber agreement,” *Reuters* (30 Sept 2015). (3 pages) <http://www.reuters.com/article/2015/09/30/us-usa-cybersecurity-idUSKCN0RT1Q820150930> **Online**

Marine Corps University / Command and Staff College
The Electives Program

(g) Timothy L. Thomas, "Google Confronts China's 'Three Warfares'," *Parameters* (Summer 2010), pp. 101-113. (13 pages)
<http://www.carlisle.army.mil/USAWC/parameters/Articles/2010summer/Thomas.pdf>

Online

(h) Various intelligence products

(3) Supplemental Reading:

(a) Singer & Friedman, pp. 91-96, 138-144 (11 pages)

(b) Mandiant, *APT1: Exposing One of China's Cyber Espionage Units* (19 Feb 2013), pp. 1-60, skim remainder (60 pages)

http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

(c) Keir Giles & William Hagestad II, "Divided by a Common Language: Cyber Definitions in Chinese, Russian and English," in *Proceedings of the 5th International Conference on Cyber Conflict*, K. Podins, J. Stinissen, M. Maybaum (eds.) (2013). (15 pages) https://ccdcoe.org/publications/2013proceedings/d3r1s1_giles.pdf

(4) Issues for Consideration:

(a) How do relations on cyber issues affect the larger U.S./China relationship?

(b) Does it make sense to distinguish between different types of espionage (i.e., national security and economic)? What are the implications of doing so? Can espionage be escalatory in international relations?

(c) Are China's views on information and espionage logical and defensible in a global context?

d. Class 4, 5 February 2016, *International Law Applicable to Cyber Warfare*

The application of international law, especially the law of armed conflict, to issues of cyber conflict.

(1) Required Reading (45 pages):

(a) Remarks of Harold Hongju Koh, Legal Advisor, U.S. Department of State, at USCYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (19 Sept 2012). (7 pages) <http://www.state.gov/s/l/releases/remarks/197924.htm> **Online**

(b) Singer & Friedman, pp. 120-133. (13 pages) **Blackboard**

(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), pp. 13-31, 39-40. (20 pages)
<http://www.jag.navy.mil/documents/navylawreview/NLRVolume60.pdf> **Online**

(d) Kyle Genaro Phillips, "Unpacking Cyberwar: The Sufficiency of the Law of Armed Conflict in the Cyber Domain," *Joint Forces Quarterly*, Issue 70, 3rd Quarter 2013, pp. 70-75. (5 pages) http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-70/JFQ-70_70-75_Phillips.pdf **Online**

(2) Supplemental Reading:

(a) Cordula Droege, "No Legal Vacuum in Cyber Space," International Committee of the Red Cross, *Resource Centre* (16 Aug 2011) (2 pages)
<https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm>

(b) NATO, Cooperative Cyber Defense Centre of Excellence, *The Tallinn Manual*, Tallinn, Estonia (Cambridge University, 2013), pp. 54-61, 106-110. (12 pages)
<http://www.ccdcoe.org/249.html>

Marine Corps University / Command and Staff College
The Electives Program

(c) Matthew C. Waxman, "Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions," *International Law Studies*, Vol. 89 (2013), pp. 109-122 (15 pages) <http://www.usnwc.edu/getattachment/8da8759f-6a32-419d-b813e7f4f1ec5a62/Waxman.aspx>

(d) Michael N. Schmitt, "Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of Int'l. Law*, Vol. 54 (2014), pp. 697-732. (35 pages)
http://www.vjil.org/assets/pdfs/vol54/Schmitt-v7-JRN_FINAL_TO_PUBLISH.pdf

(3) Issues for Consideration:

(a) What is a cyber war? Why do we care if it's called a war?

(b) How different are the laws governing cyber warfare than past laws governing warfare? How different is it to apply LOAC to cyber warfare? Is LOAC sufficient?

e. Class 5, 9 February 2016, Threat & Response 2: Russia

Russia's activities in cyber and how they relate to Russian kinetic activities and national strategy.

(1) Required Reading (51 pages):

(a) Jeff Carr, ed., *Project Grey Goose Phase II Report: The evolving state of cyber warfare* (20 Mar 2009), pp. 15-23. (8 pages)
<http://ferror.com/pdf/GreyGoose2.pdf> **Online**

(b) Adrian Chen, "The Agency," *New York Times Magazine* (2 June 2015). (13 pages) http://www.nytimes.com/2015/06/07/magazine/the-agency.html?_r=2
Online

(c) Eneken Tikk, Kadri Kaska & Liis Vihul, *International Cyber Incidents, "Estonia 2007"* (2010), pp. 14-25, 33 (pp. 25-32 optional). (12 pages) **Blackboard**

(d) Daisy Sindelar, *The Atlantic*, "The Kremlin's Troll Army" (12 Aug 2014). (7 pages) <http://www.theatlantic.com/international/archive/2014/08/the-kremlins-troll-army/375932/> **Online**

(e) Margaret Coker & Paul Sonne, "Ukraine: Cyberwar's Hottest Front," *Wall Street Journal* (10 Nov 2015). (4 pages) **Blackboard**

(f) 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> **Online**

(g) Various intelligence products

(2) Supplemental Reading:

(a) David M. Hollis, "Cyber War Case Study, Georgia 2008," *Small Wars Journal*, 6 Jan 2011. (10 pages) <http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008>

(b) Jeffrey Carr, *Inside Cyber Warfare*, 2d ed., (2012), pp. 15-19, 103-119.

(c) *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. (6 pages)

<https://ccdcoe.org/sites/default/files/documents/UN-150113-CodeOfConduct.pdf>

Marine Corps University / Command and Staff College
The Electives Program

(d) Timothy L. Thomas, "Russian Views on Information-based Warfare," *Airpower Journal* (Jul 1996). (9 pages)
<http://fmso.leavenworth.army.mil/documents/rusvuiw.htm#9a> .

(3) Issues for Consideration:

(a) Were the Russian cyber attacks in Estonia & Georgia a tactical success? A strategic success?

(b) Is Russia making effective use of social media to advance its national interests?

(c) Do Russian cyber activities represent a new kind of warfare, or are they just a continuation of the Western way of war?

f. Class 6, 11 February 2016, US Policy & Law Framework

Aspects of the complex legal system in the U.S. and how it applies to cyber operations.

(1) Required Reading (36 pages):

(a) Stewart Baker, "What is the Role of Lawyers in Cyberwarfare?" *ABA Journal* (1 May 2012) (4 pages)
http://www.abajournal.com/magazine/article/what_is_the_role_of_lawyers_in_cyberwarfare/ **Online**

(b) *International Strategy for Cyberspace* (May 2011), pp. 9-14. (5 pages)
https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf **Online**

(c) DoD Law of War Manual (Jun 2015), pp. 994-1009. (15 pages)
<http://www.defense.gov/Portals/1/Documents/pubs/Law-of-War-Manual-June-2015.pdf> **Online**

(d) Gary Brown, "Cyber Conflict in DOD's Law of War Manual," *Just Security* (27 Jul 2015). (4 pages) <https://www.justsecurity.org/24950/cyber-conflict-dods-law-war-manual/> **Online**

(e) Charlie Dunlap, "Cyber Operations and the New Defense Department Law of War Manual: Initial Impressions," *Lawfare* (15 Jun 2015). (8 pages)
<https://www.lawfareblog.com/cyber-operations-and-new-defense-department-law-war-manual-initial-impressions#> **Online**

(f) Various classified documents

(2) Supplemental Reading:

(a) None

(3) Issues for Consideration:

(a) Should one agency own the cyber mission, or should it be divided across government? How?

(b) Should the U.S. do more to signal and disclose its cyberspace activities?

g. Class 7, 17 February 2016, Military Doctrine, Strategy & Role

DoD organization, guidance and strategy in the context of the U.S. government and the international community.

(1) Instructor: MFCY/CG

(2) Required Reading (52 pages):

(a) *MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept*, 1 May 2014 (FOUO), pp. 2-18 (16 pages) **Blackboard**

Marine Corps University / Command and Staff College
The Electives Program

(b) Ervin J. Rokke, Thomas A. Drohan & Terry C. Pierce, “Combined Effects Power,” *Joint Forces Quarterly*, No. 73, 2d Quarter, 2014. (6 pages)

<http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577501/jfq-73-combined-effects-power.aspx> **Online**

(c) DoD Cyber Strategy (Apr 2015), pp. 17-28. (11 pages)

http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf **Online**

(d) JP 3-12 (R), *Cyberspace Operations* (5 Feb 2013), pp. II 1-12; III 1-2, 10; IV 3, 6-8. (19 pages)

(e) Various classified documents

(3) Supplemental Reading:

(a) None

(4) Issues for Consideration:

(a) What’s the right C2 model for cyberspace forces? Is it different than the traditional model?

(b) Is there a need for Service-specific cyberspace missions?

h. Class 8, 19 February 2016, Threat & Response 3: Iran

Iran’s activities in cyberspace, plus the broader implications of Stuxnet to international relations and military operations.

(1) Required Reading (66 pages):

(a) Kim Zetter, “Olympic Games,” *Countdown to Zero Day* (2014), pp. 308-335, 371-405. (62 pages) **Blackboard**

(b) Melissa Clyne, “Iran Poses Cyberthreat to US Firms, Infrastructure: State Dept,” *NewsMax* (12 May 15). (2 pages) <http://www.newsmax.com/Newsfront/iran-cyber-threat-businesses/2015/05/12/id/644010/>

(c) Gary D. Brown, “Why Iran Didn’t Admit Stuxnet Was an Attack,” *JFQ*, Issue 63 (4th Quarter 2011), pp. 70-73. (4 pages)
<http://lomc.idm.oclc.org/login?url=http://search.proquest.com/docview/926433852?accountid=14746>

(d) Various classified documents

(2) Supplemental Reading:

(a) Jon R. Lindsay, “Stuxnet and the Limits of Cyber Warfare,” *Security Studies*, Vol. 22, No. 3 (2013), pp. 365-404. (39 pages)

<http://www.tandfonline.com/doi/pdf/10.1080/09636412.2013.816122>

(3) Issues for Consideration:

(a) Was the Stuxnet attack successful? Was it an act of war?

(b) Was it legal? What would it have taken to justify Stuxnet under international law?

(c) What is the relationship between Stuxnet and Iran’s cyber responses, and the politics of nuclear weapons?

i. Class 9, 23 February 2016, Big Data, Social Media and Information as Power

The amount of available information, as well as the speed with which it can be distributed, has created threats and opportunities in national security.

(1) Location: MCIA

(2) Instructor:

Marine Corps University / Command and Staff College
The Electives Program

(3) Required Reading (69 pages):

(a) John Reed, “‘Internet in a Suitcase’ Ready for Field Testing,” *Foreign Policy* (5 Nov 2012). (3 pages) <http://foreignpolicy.com/2012/11/05/internet-in-a-suitcase-ready-for-field-testing/> **Online**

(b) Bruce Schneier, *Data and Goliath* (2015), pp. 20-45. (25 pages)

Blackboard

(c) 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/#> **Online**

(d) Steven Metz, “The Internet, New Media, and the Evolution of Insurgency,” *Parameters*, Vol. XLII, No. 3 (Autumn 2012), pp. 80-90. (10 pages) <http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2012autumn/Metz.pdf> **Online**

(e) Victor D. Cha and Nicholas D. Anderson, “A North Korean Spring.” *The Washington Quarterly* Vol. 35, No. 1 (2012), pp. 7-24. (17 pages) <http://www-tandfonline-com.lomc.idm.oclc.org/doi/pdf/10.1080/0163660X.2012.641728> **Online**

(f) Singer & Friedman, pp. 108-114. (6 pages)

(4) Supplemental Reading:

(a) United States Institute of Peace, “New Media and Conflict after the Arab Spring,” *Peaceworks* 80 (2012): 1-24. (24 pages) <http://www.usip.org/sites/default/files/PW80.pdf>

(b) Dubai School of Government, “Civil Movements: The impact of Facebook and Twitter,” Arab Social Media Report, Vol. 1 No. 2 (May 2011), p. 1-30. (30 pages) <http://unpan1.un.org/intradoc/groups/public/documents/dsg/unpan050860.pdf>

(5) Issues for Consideration:

(a) How important are big data and social networking to warfare?

(b) Did social networking cause or enable the Arab Spring? Will it have the same effect elsewhere? Is this a good thing or a bad thing?

(c) What are the risks to the military of big data? What are the benefits?

j. Class 10, 26 February 2016, *Deterrence, Norms and the Future of Cyber Operations*

Some other lines of inquiry regarding cyberspace operations, and a discussion of possible future directions.

(1) Required Reading (73 pages):

(a) Ervin J. Rokke, Thomas A. Drohan & Terry C. Pierce, “Combined Effects Power,” *Joint Forces Quarterly*, No. 73, 2d Quarter, 2014. (6 pages) <http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/577501/jfq-73-combined-effects-power.aspx>

(b) Henry Rõigas and Tomáš Minárik, “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,” *Incyder News* (31 Aug 15). (3 pages) <https://ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html>

(c) Will Goodman, “Cyber Deterrence: Tougher in Theory Than in Practice,” *Strategic Studies Quarterly* (Fall 2010), pp. 102-135. (33 pages) **Blackboard**

Marine Corps University / Command and Staff College
The Electives Program

(d) Eric Sterner, “Retaliatory Deterrence in Cyberspace,” *Strategic Studies Quarterly* (Spring 2011), pp. 62-80. (18 pages) **Blackboard**

(e) Singer & Friedman, pp. 96-106, 144-147. (13 pages) **Blackboard**

(2) Supplemental Reading:

(a) David C. Benon, “Why the Internet Is Not Increasing Terrorism,” *Security Studies*, Vol. 23, No. 2 (2014), pp. 293-328. (35 pages)

<http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/2012autumn/Metz.pdf>

(3) Issues for Consideration:

(a) Is the Cold War a model for cyber deterrence? What should deterrence look like in cyberspace? Is it possible or desirable?

(b) Does cyber deterrence reinforce or detract from international cyber norms?

(c) Are norms a viable model for controlling behavior in cyberspace?

5. Student Requirements.

Students must read the assigned readings, contribute to scheduled seminars, conduct a seminar presentation, and write a course paper.

a. Seminar Presentation. One oral presentation in seminar from a list of cyber readings. A presentation consists of a 5-minute talk in which the student presents their analysis of the reading and conducts a 5-10 minute Q&A session in which the student leads a discussion of the issues for consideration they have presented.

b. Course Paper. An analysis of one aspect of cyber warfare. The course paper is due at the final seminar and should be five to seven pages in length. Your paper should be double-spaced, with one-inch margins, prepared in 12-point pitch, Times New Roman font, with endnotes and a bibliography.

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.

Lesson Hours:

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

Marine Corps University / Command and Staff College
The Electives Program

Submitted by:

Reviewed and Approved:

ERIC Y. SHIBUYA, PH.D.
ELECTIVES COORDINATOR

CHARLES D. MCKENNA, PH.D.
DEAN OF ACADEMICS

“I have reviewed this material and it is in conformance with MCU Policy Letter 04-06,
use of copyrighted material.”

EDWARD J. ERICKSON, PH.D.
COPYRIGHT CONTROL MANAGER

DATE