American Public University System

The Ultimate Advantage is an Educated Mind

School of Security and Global Studies
INTL647
Cyber Intelligence
Credit Hours: 3
Length of Course: 8 Weeks
Prerequisite:INTL500

Table of Contents

Course Description (Catalog)

INTL647 (3 credit hours). This course is a study of Cyber Intelligence from its nascent stages to its current operational and policy impact. Students will explore the full range of cyber capabilities from exploitation to defense including several case studies that demonstrate the challenges and benefits of cyber intelligence operations. The course will demonstrate how cyber has changed the nature of intelligence collection, operations, and analysis across the US Intelligence and Defense communities.

Table of Contents

Course Scope

This course focuses on specialized area knowledge and sources in the field.

Table of Contents

Course Objectives

After successfully completing this course, you will be able to:

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

- CO1: Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.
- CO2: Assess the attributes of computer network exploitation, defense and attack within the intelligence context.
- CO3: Examine the intelligence challenge of attribution in cyber-attacks.
- CO4: Evaluate the benefits and risks of the current cyber intelligence structure in the US.
- CO5: Analyze the legal and policy challenges in the conduct of cyber intelligence operations.

Table of Contents

Course Delivery Method

This course, delivered via distance learning, will enable students to complete academic work in a flexible manner, completely online. Course materials and access to an online learning management system will be available to each student. Online assignments are due by ***Sunday at 11:55 pm ET*** and include all written assignments, examinations, and research papers submitted for grading. Weekly Forum questions (accomplished in groups in a Forum) require an initial response by ***Thursday at 11:55 pm ET***, with all other required responses due by ***Sunday at 11:55 pm ET***. The assigned faculty will support the students throughout this eight-week course.

Table of Contents

Course Resources

Required Course Textbooks. The required text for this course is:

- Reveron, Derek S. 2012. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* Georgetown University Press.

Required Readings

- External websites and other assigned readings are found in the Lessons area of the classroom.
- Weekly Lesson Notes and videos or audio files are found in the Lessons area of the classroom.

Table of Contents

Evaluation Procedures

The course grade is based on the following assessments:

Discussion Forums – 15 percent

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Discussion questions will be provided and posts should reflect an assimilation of the readings and respond to the assigned topic(s). Students are required to provide a substantive initial post by ***Thursday at 11:55 pm ET and respond to two or more classmates by Sunday 11:55 pm ET***. Forum posts are graded on timeliness, relevance, knowledge of the weekly readings, and the quality of original ideas.

Cyber White Paper – 20 percent

For this assignment, you will select a topic or issue as it relates to cyber space and the challenges associated with it. This white paper will form as the basis for developing a Cyber Research Proposal (**Assignment #2**) and Final Paper that focuses on your selected cyber issue (**Assignment #3**). Your white paper assignment is ***4-5 pages*** in length.

Cyber Research Proposal – 30 percent

The goal of this assignment is to present a clear research proposal. Your research proposal should be between ***5-6 pages in length*** not including your preliminary source list and references.

Cyber Issue Paper – 35 percent

This assignment is a take-home essay where you are functioning as a Presidential Adviser and are tasked to prepare a ***13-15 page (double spaced) memorandum*** outlining possible courses of action in light of a fictitious Cyber Attack.

ASSIGNMENT	Percentage
Discussion Forums	**15 percent**
Cyber White Paper	**20 percent**
Cyber Research Proposal	**30 percent**
Cyber Issue Paper	**35 percent**
TOTAL	**100 percent**

Table of Contents

8 – Week Course Outline

Week 1: Introduction to Cyber Intelligence.

Learning Outcomes:

- Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.
- Assess the attributes of computer network exploitation, defense and attack within the intelligence context.

Assignments: Complete Introductory and Week 1 forum posts.

Required Readings:

Demchak, Chris C. *Studies in Security and International Affairs : Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA; The University of Georgia Press, 2011. (Chapter 1).

Intelligence and National Security Alliance (INSA), "Cyber Intelligence: Setting the Landscape For An Emerging Discipline," *INSA* (2011). Accessed at: https://images.magnetmail.net/images/clients/INSA/attach/INSA_CYBER_INTELLIGENCE_2011.pdf.

Masters, Jonathan, "Confronting the Cyber Threat," *Council on Foreign Relations*. Accessed at: http://www.cfr.org/technology-and-foreign-policy/confronting-cyber-threat/p15577

U.S. Government. Government Accountability Office (GAO). A Briefing for the Subcommittee on Emerging Threats and Capabilities, Committee on Armed Services, House of Representatives (July 29, 2011). Accessed at: http://www.gao.gov/new.items/d11695r.pdf.

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Edited by Derek S. Reverson. Washington, DC: Georgetown University Press, 2012. (Chapter 1).

Warner, Michael. "Cybersecurity: A Pre-History." *Intelligence and National Security* 27, No.5 (2012): 781-789.

Zegart, Amy B. "September 11 and the Adaptation Failure of U.S. Intelligence Agencies." *International Security* 29, No. 4 (Spring 2005), pp. 78–111. Accessed at: http://faculty.maxwell.syr.edu/rdenever/USNatSecandForeignPol/Zegart.pdf.

<u>Week 2: Military Role in Defending Computer Networks</u>.

Learning Outcomes:

- Assess the attributes of computer network exploitation, defense and attack within the intelligence context.
- Debate the benefits and risks of the current cyber intelligence structure in the US.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Assignments: Complete Week 2 forum posts.

Required Readings:

Demchak, Chris C. *Studies in Security and International Affairs : Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. Athens, GA; The University of Georgia Press, 2011. (Chapter 3).

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World,* Edited by Derek S. Reverson. Washington, DC: Georgetown University Press, 2012. (Chapters 3 and 6).

Software Engineering Institute (SEI). *Cyber Intelligence Tradecraft Project: Summary of Key Findings*, SEI Emerging Technology Center, 2013, Accessed at: http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf. (Pgs. 1-22).

U.S. Government. Department of Defense (DoD). *The DoD Cyber Strategy*. Washington, DC: Government Printing Press, 2015. Accessed at: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. (Pgs. 1-42).

Williams, Phil, Timothy Shimeall, and Casey Dunlevy, "Intelligence Analysis for Internet Security," *Contemporary Security Policy* 23, no.2 (2013), pp. 1-38.

Shanker, Thom. "Pentagon Is Updating Conflict Rules in Cyberspace." *New York Times* (New York, NY), June 27, 2013. Accessed at: http://www.nytimes.com/2013/06/28/us/pentagon-is-updating-conflict-rules-in-cyberspace.html?_r=0.

Week 3: Challenges to Attribution - The Estonia Case Study.

Learning Outcomes:

- Examine the intelligence challenge of attribution in cyber-attacks.

Assignments: Complete Week 3 forum posts.

Required Readings:

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Clark, David D. and Susan Landau, "Untangling Attribution," *Harvard National Security Journal* (2011), pp. 1-30. Accessed at: http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf.

Hare, Forrest. "The Significance of Attribution to Cyberspace Coercion: A Political Perspective." 4th International Conference on Cyber Conflict (2012), pp. 1-15. Accessed at: https://ccdcoe.org/cycon/2012/proceedings/d2r1s2_hare.pdf.

Healey, Jason, "Beyond Attribution: Seeking National Responsibility for Cyber Attacks," *Atlantic Council Issue Paper*, Cyber Statecraft Initiative (2011), pp. 1-8. Accessed at: http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF.

Lewis, James A., "Cyber Attacks Explained," Center for Strategic and International Studies (2007), pp. 1-2. Accessed at: http://www.mafhoum.com/press10/302T42.pdf.

Rid, Thomas and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (2015), pp. 4-37. Accessed at: https://sipa.columbia.edu/system/files/Cyber_Workshop_Attributing%20cyber%20attacks.pdf.

Traynor, Ian, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian* (17 May 2007). Accessed at: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

Shackleford, Scott J. "State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem." Conference on Cyber Conflict (2010). Accessed at: https://ccdcoe.org/sites/default/files/multimedia/pdf/Shackelford%20-%20State%20Responsibility%20for%20Cyber%20Attacks%20Competing%20Standards%20for%20a%20Growing%20Problem.pdf.

Waterman, Shaun, "Who Cybersmacked Estonia?" UPI, June 11, 2007. Accessed at: http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439/.

Week 4: Legal Issues.

Learning Outcomes:

- Analyze the legal and policy challenges in the conduct of cyber intelligence operations.

Assignments: Complete Week 4 forum posts and submit your Cyber White Paper.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Required Readings:

Chesney, Robert, Military-Intelligence Convergence and the Law of the Title 10/Title 50 Debate," *Journal of National Security Law and Policy* 539 (2012). Accessed at: http://jnslp.com/wp-content/uploads/2012/01/Military-Intelligence-Convergence-and-the-Law-of-the-Title-10Title-50-Debate.pdf.

Finklea, Kristin and Catherine A. Theohary. *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*. Washington, DC: Congressional Research Service, 2015. (Pages 1-31). Accessed at: https://www.fas.org/sgp/crs/misc/R42547.pdf.

Lie, Edward C. *Cybersecurity: Selected Legal Issues*. Washington, DC: Congressional Research Service, 2012. (Pages 1-31).

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Edited by Derek S. Reverson. Washington, DC: Georgetown University Press, 2012. (Chapter 5).

Williams, Robin D., "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action," *The George Washington Law Review* 79, No. 1162. Accessed at: http://www.gwlr.org/wp-content/uploads/2012/08/79-4-R_Williams.pdf.

Week 5: Cyber Threats.

Learning Outcomes:

- Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.

Assignments: Complete Week 5 forum posts.

Required Readings:

Clapper, James R., "U.S. Intelligence Community: Worldwide Threat Assessment" *Statement for the Record*, February 9, 2016 (see section on Cyber and Technology). pp. 1-4. Accessed at: https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf.

McWhorter, Dan, "Exposing One of China's Cyber Espionage Units," *Mandiant Intelligence Center Report* (February 19, 2013), pp. 1-2. Accessed at: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Office of the National Counterintelligence Executive. Foreign Spies Stealing US Economic Secrets in Cyberspace (October 2013). Accessed at: https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Edited by Derek S. Reverson. Washington, DC: Georgetown University Press, 2012. (Chapter 4). Pages 57-71.

Singer, Peter.W., "The Cyber Terror Bogeyman," *The Brookings Institut*e (November 1, 2012). pp. 1-4. Accessed at: https://www.brookings.edu/articles/the-cyber-terror-bogeyman/

Symantec. Internet Security Threat Report (ISTR), 2015. pp.1-120. Accessed at: https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf

Week 6: Social Media and Open Source Intelligence (OSINT).

Learning Outcomes:

- Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.

Assignments: Complete Week 6 forum post and submit your Cyber Research Proposal.

Required Readings:

Hodges, Jim "OSINT Goes Social," *Trajectory Magazine* (Fall 2012). Accessed at: http://trajectorymagazine.com/civil/item/1307-osint.html.

Omand, David, "Introducing Social Media Intelligence (SOCMINT)," *Intelligence and National Security* 27, No. 6, pp. 801–823.

Waters, T.J., "Social Media and the Arab Spring," *Small Wars Journal* (November 14, 2012) Accessed at: http://smallwarsjournal.com/jrnl/art/social-media-and-the-arab-spring.

Moe, Wendy W. and David A. Schweidel. *Social Media Intelligence*. New York, NY: Cambridge University Press, 2015. (Chapter 1, Chapter 9, Chapter 10)

Zeng, David, Hsinchun Chen, Robert Lusch, and Shu-Hsing Li. "Social Media Analytics and Intelligence." *IEEE Intelligent Systems* 25, No.6, pp.13-16.

Week 7: Return to Cyber War.

Learning Outcomes:

- Examine the history and development of cyber intelligence operations and how those operations can integrate with other intelligence collection.

Assignments: Complete Week 7 forum posts.

Required Readings:

Arquilla, John, "Cyber War Is Already Upon Us," *Foreign Policy* (March/April 2012). Accessed at: http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us.

Butler, Mark C., "Refocusing Cyber War Thought," *Air & Space Power Journal* 27, No.27 (2013), pp. 44-57.

"Debate: Has Cyber War Been Exagerated?" Intelligence Squared, National Public Radio (June 2010), podcast and transcript available at: http://www.npr.org/templates/story/story.php?storyId=127861446.

Rid, Thomas, "Think Again: Cyber War," *Foreign Policy* (March/April 2012). Accessed at: http://foreignpolicy.com/2012/02/27/think-again-cyberwar/.

Solis, Gary D., "Cyber Warfare," *Military Law Review* 219 (2014), pp. 1-52.

Week 8: Future Policy and Legislative Issues.

Learning Outcomes:

- Debate the benefits and risks of the current cyber intelligence structure in the US.
- Analyze the legal and policy challenges in the conduct of cyber intelligence operations.

Assignments: Complete Week 8 forum posts and submit your Cyber Issue Paper.

Required Readings:

The Cyber Intelligence Sharing and Protection Act (CISPA): Another SOPA, *National Security Law Brief*, Washington College of Law. Accessed

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

at: http://nationalsecuritylawbrief.com/the-cyber-intelligence-sharing-and-protection-act-cispa-another-sopa/.

U.S. Government. House of Representatives. *Cyber Intelligence Sharing and Protection Act*. Accessed at: http://www.govtrack.us/congress/bills/113/hr624/text.

Flowers, Angelyn and Sherali Zeadally, "US Policy on Active Cyber Defense," *Homeland Security & Emergency Management* 11, No. 2 (2014), pp. 289-308.

Dunn Cavelty, Myriam, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics* 20, No. 3 (Sep 2014), pp. 701-15.

Table of Contents

Policies

Please see the Student Handbook to reference all University policies. Quick links to frequently asked question about policies are listed below.

Drop/Withdrawal Policy

Plagiarism Policy

Extension Process and Policy

Disability Accommodations

Citation and Reference Style

Attention Please: Students will follow the Turabian/Chicago Style as the sole citation and reference style used in written work submitted as part of coursework to the University.

See http://www.apus.edu/Online-Library/tutorials/chicago.htm.

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. A Late Penalty of ***5% per day*** will be assessed for late work. As adults, students, and working professionals, I understand you must manage competing demands on your time. Should you need additional time to complete an assignment, please contact me before the due date so we can discuss the situation and determine an acceptable resolution.

Netiquette

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

Online universities promote the advancement of knowledge through positive and constructive debate – both inside and outside the classroom. Forums on the Internet, however, can occasionally degenerate into needless insults and "flaming." Such activity and the loss of good manners are not acceptable in a university setting – basic academic rules of good behavior and proper "Netiquette" must persist. Remember that you are in a place for the rewards and excitement of learning which does not include descent to personal attacks or student attempts to stifle the Forum of others.

- Technology Limitations: While you should feel free to explore the full-range of creative composition in your formal papers, keep e-mail layouts simple. The Sakai classroom may not fully support MIME or HTML encoded messages, which means that bold face, italics, underlining, and a variety of color-coding or other visual effects will not translate in your e-mail messages.
- Humor Note: Despite the best of intentions, jokes and especially satire can easily get lost or taken seriously. If you feel the need for humor, you may wish to add "emoticons" to help alert your readers: ;-), :), ☺

Table of Contents

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to librarian@apus.edu.

- *Charles Town Library and Inter Library Loan:* The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- *Electronic Books:* You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- *Electronic Journals:* The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.

Request a Library Guide for your course (http://apus.libguides.com/index.php)

The AMU/APU Library Guides provide access to collections of trusted sites on the Open Web and licensed resources on the Deep Web. The following are specially tailored for academic research at APUS:

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

- Program Portals contain topical and methodological resources to help launch general research in the degree program. To locate, search by department name, or navigate by school.
- Course Lib-Guides narrow the focus to relevant resources for the corresponding course. To locate, search by class code (e.g., SOCI111), or class name.

If a guide you need is not available yet, please email the APUS Library: librarian@apus.edu.

Table of Contents

Turnitin.com

Faculty require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. The instructor will post information in the classroom on student procedures.

Table of Contents