

19 August 2019

Subj: SY403 COURSE POLICY-AY2020 Fall

Ref: (a) ACDEANINST 1531.58, Administration of Academic Programs
(b) ACDEANINST 1531.64, Academic Accountability
(c) CYBSCIINST 3120.32, Cyber Science Department Standard Organization and Regulations Manual
(d) ACDEANNOTE 1531, Academic Scheduling and Start of Semester Items

1. Purpose: Per references (a) through (d), the following comprises the course policies for SY403 - **National Security Decision Making in the Cyber Age**, AY2020 Fall term.

2. General Information:

Course: SY403 - National Security Decision Making in the Cyber Age

Credits: 3

Term: AY2020 Fall

Prerequisites: None

3. Course Description: This course is intended to prepare midshipmen to understand the characteristics of all aspects of cyber power and the role of national security decision makers in a world increasingly influenced by cyber power. It does so by presenting them with emerging conceptual, strategic, policy, legal, ethical, organizational, and operational aspects of cyber power, with particular attention to military and naval aspects. The course will convey the current body of knowledge regarding cyber power. However, because that knowledge is and will remain fluid, priority will be on the development of analytic skills. Thus, *what to know* about cyber power will be combined with *how to think* about cyber power. Once introduced to key aspects and issues of cyber power, students will be presented with decision-making exercises, simulations, and research tasks to apply and develop such analytic skills. The course will deal with cyber offensive and defensive challenges and with the full range of potential adversaries. Basic familiarity with computer-network security and national-security affairs is expected.

4. Course Learning Outcomes: SY403 is designed to support the following Learning Outcomes (as indicated in the August 2017 Cyber Science Department matrix of Required Cyber Operations Course Learning Outcomes):

- “3. An ability to communicate effectively with a range of audiences about technical Information” through:
 - Verbal Communication
 - Written Communication
- “4. An ability to make informed judgments in computing practice based on legal and ethical principles”, through explicit coverage of:
 - Legal Principles
 - Ethical Principles

- Making Judgements
- “5. An ability to function effectively on teams to establish goals, plan tasks, meet deadlines, manage risks and produce deliverables”, through the use of:
 - Team Dynamics
- “6. An ability to apply security principles and practices to the environment, hardware, software, and human aspects of a system.” Explicitly covering:
 - Confidentiality
 - Integrity
 - Availability
 - Risk
 - Adversarial Thinking
- “7. An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.” Covering:
 - Offensive Cyber Operations
 - Defensive Cyber Operations

With those learning outcomes, in mind, this course has been designed to help students develop an understanding of, and be able to apply, the following:

- Types and levels of cyber-power threats to national security
- U.S. uses of cyber power to achieve success in military and other operations
- Linkages between different types/levels of cyber threats and US national and international interests and responses;
- Foundational US policies and legal considerations as they relate to both national and international cyber activities;
- Public policy issues and how they affect the application of cyber power;
- Application of basic concepts of conflict and warfare as they relate to cyber power;
- US Government organization for offensive and defensive cyber power, focusing on DoD;
- Options for mitigating the vulnerabilities and exploiting the benefits of cyberspace in the face of threats;
- How cyber power and conventional military power can integrate with one another.
- Applications of cyber power on Navy/Marine Corps, joint, and coalition operations.

Unlike the more robust bodies of thought and established norms for both conventional kinetic weapons and weapons of mass destruction, the analogous literature for cyber matters is, to a large extent, relatively new and undeveloped. In a similar vein, the course will spend a good deal of time considering how the United States has chosen to respond to the cyber situation to date, and will also explore alternative ideas and structures. Students will be asked to read a number of current policy documents and related materials, and to ultimately put these ideas together as they’re applied today, as well as how they might be changed in the future.

Guest Speakers: The course will have subject matter experts interact with the class during the semester. These individuals will bring additional and new perspectives on national security cyber-related matters, and students should come prepared to listen, learn from, and challenge each of them. The Professor will notify the class in advance of these opportunities.

5. Course Resources:

- a. The most important resource will be a student's individual effort as demonstrated in accomplishing the readings, working through the questions for each lesson and devoting sufficient time to required research and assigned writing assignments.
 - b. Readings are to be accomplished prior to the lesson in which they will be discussed.
 - c. In general, students will find the reading materials for this course in several places.
- Current periodicals, policies, and papers. This collection of assigned reading materials is available on the course web site:
<http://rona.academy.usna.edu/~inglis/sy403lect2017.php>
 - Assigned readings are keyed to topics in the syllabus.
 - **Required** readings for each lesson are listed on the SY403 website and are sourced from cyber policy, academic research and contemporary reports on various cyber topics. These are testable and will be the subject of classroom discussion on the day they are assigned.
 - **Supplemental** readings are intended to complement classroom discussion and to serve as a foundation for further research and study (e.g., for student written Assignments 1, 2 and 3)
 - Books
 - The following are recommended as supplemental reading for this course and serve as sources for written assignments referred to as Assignments 1, 2 and 3:
 - Buchanan, Ben, ***The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations***, Oxford, New York, Oxford University Press, 2015
 - Clarke, Richard A. and Knake, Robert K., ***The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats***, New York, Penguin Press, 2019
 - Clarke, Richard A. and Knake, Robert K., ***Cyber War***, New York, Harper Collins, 2010 (referred to in the syllabus as "Clarke")
 - Corera, Gordon, ***Cyber Spies – The Secret History of Surveillance, Hacking and Digital Espionage***, New York, London, Pegasus, 2015
 - Kaplan, Fred, ***Dark Territory – The Secret History of Cyber War***, New York, Simon and Schuster, 2016
 - Klimburg, Alexander ***The Darkening Web – The War for Cyberspace***, New York, Penguin Press, 2017
 - Libicki, Martin C., ***Cyberspace in Peace and War***, Annapolis, Naval Institute Press, 2016

- Sanger, David E, *The Perfect Weapon – War Sabotage and Fear in the Cyber Age*, New York, Crown Books, 2018
- Segal, Adam *The Hacked World Order – How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, New York, PublicAffairs (A Council on Foreign Relations book), 2016-7
- Singer, P.W. and Cole, August *Ghost Fleet*, Boston, New York, Houghton Mifflin Harcourt, 2015
- Singer, P.W. and Brooking, Emerson T, *LikeWar – The Weaponization of Social Media*, Boston, New York, Houghton Mifflin Harcourt, 2018.
- Singer, P.W. and Friedman, Allan *Cybersecurity and Cyberwar – What Everyone Needs to Know*, Oxford, Oxford University Press, 2014 (Referred to in the syllabus as “Singer”)
- Wittes, Benjamin and Blum, Gabriella *The Future of Violence*, New York, Basic Books, 2015

6. Grading:

- a. Every effort will be made to ensure prompt and substantive feedback on graded material. Feedback and grades will be clearly marked on returned work.
- b. Assignments: Are due as indicated in the course syllabus. Assignments submitted after due dates without prior permission of the instructor will be decremented one letter grade per class period until submitted to the instructor. Regardless of the grade on a given task, all assignments must be completed to receive a final grade in the course.
- c. Tests: An in-class test will be given at six weeks. There will be an in-class final exam. All exams are cumulative.
- d. Simulations and Briefings: These scenario-based exercises will be an opportunity for students to put into practice what they have learned in theory. They will be conducted during the latter part of the term, with one involving a national-level scenario and the other a more military/operational scenario. In preparation for the December exercise, students are asked to prepare a short paper (Assignment 2, 5-7 pages in length) and a proposed course of action to help prepare for a role in the simulation (Assignment 3). Grades will be assigned based on a combination of the paper and individual game and/or briefing participation.
- e. Weighting of the course grade will be as follows:
 - Six Week Exam: 20%
 - Final Exam: 30%
 - Homework and writing assignments 20%
 - Includes individual effort papers referred to as *Assignment 1* (due 15 October 2019), *Assignment 2* (your chosen thesis statement is due on 22 October 2019 with the full assignment due 29 October 2019) and *Assignment 3* (due 26 November 2019)
 - Simulation/Briefings: 15%
 - Class Participation: 15%

7. Honor policy: The following collaboration policies shall apply to the assignments specified. When in doubt, students should seek clarification from their instructor.

- Homework readings: Students are encouraged to freely discuss the readings assigned and their implications.
- Written assignments turned in for grades (to include Assignments 1, 2 and 3): These will be the work of the given student alone. Students are permitted to discuss the meaning of the assignment but should ensure that the work they submit for grading is their original work, or properly cited with attribution to others as appropriate to the task at hand. Copying will never be considered as collaboration or discussion; copying will always be considered as a violation of the honor policy. Discussion of the application of this policy to a given assignment with a course Instructor is always allowed.
- Exam: These will be the work of that student alone. Student questions regarding the meaning or import of a particular exam problem should be addressed to the test proctor alone.

8. Other

Instructor Absence: Should an instructor fail to be present for a class within 5 minutes of the class start time, the section lead should call the Education Technician for the Cyber Department, Erin Montagnet (410-293-0930), located in Leahy room 101. They will contact the instructor staff and provide directions to the section lead.

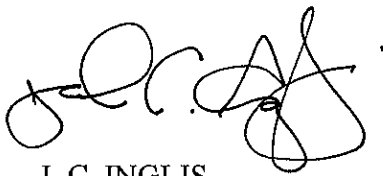
Classroom Computers: Students are required to bring a government issued laptop sufficiently charged or additionally bring a laptop battery charger to every class meeting. Students will make use of a laptop in many class meetings, to include accessing the course website for learning materials and readings. Students will be marked as “late” if they have to return to their room to retrieve a laptop or laptop battery charger.

Course Conduct

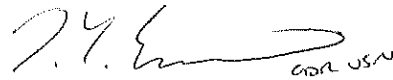
- All requirements for the course (e.g., tests, projects, participation, etc.) must be completed to complete the course successfully.
- No papers or other materials that have been used for other courses may be used for this course.
- Students must be present on the day they are assigned to participate in a simulation or make an in-class presentation. If absent without prior permission, a student may receive a “zero” for that assignment.
- Plagiarism: Midshipmen are persons of honor and integrity. As such, plagiarism is anathema to their way of life. It will not be tolerated in this course, and will result in a “zero” for the assignment and reporting to the appropriate authorities. Please see the materials at the Nimitz Library website (<http://libguides.usna.edu/plagiarism>) for further explanation. Students should check with the Professor should you have any questions about this.

Big Rules

- (1) The most current version of the Syllabus and other key course reference documents will be available on the course director's Home Page (<http://rona.academy.usna.edu/~inglis/>). All other versions should be considered obsolete.
- (2) Students should not modify, delete, or otherwise change the course readings, which will be in the same folder. Students desiring a copy of a document should COPY IT from the file onto their own computer.
- (3) This course *does* present the students with a lot of reading material. Much of it will be testable and is clearly marked as such. All of it will be valuable to the student's understanding of cyber issues that affect both professional and personal lives.
- (4) Students should read for context, synthesis, and as a basis for in-class discussion, not details.



J. C. INGLIS
SY403 Course Director



T. EMMERSEN, CDR, USN
Chair, Cyber Science Department