**National Security Decision Making in the Cyber Age**
**Course Description, Objectives, Policies and Syllabus**
**SY403**
**Fall 2019**
**U.S. NAVAL ACADEMY**

19 August 2019

Department: US Naval Academy Cyber Department and US Naval Academy Cyber Center

Instructors: Chris Inglis, Visiting Professor for Cyber Studies; Rick Ledgett, Visiting Professor for Cyber Studies; Jeff Kosseff, Assistant Professor for Cyber Studies

Class Time/Classroom:

Section 1201 (Inglis/Ledgett): Tuesday (MI200) and Thursday (MI212) 0755-0910 hrs
Section 3401 (Kosseff): Tuesday (MI294) and Thursday (MI202) , 0955-1110 hrs
Section 5601 (Kosseff): Tuesday (MI294) and Thursday (MI202), 1330-1445 hrs

Office: Professor Inglis, Leahy room 301; Phone: (410) 293-0932
Professor Kosseff, Leahy room 301; Phone: (410) 293- 0950
Professor Ledgett, Leahy room 305; Phone (410) 293-0931

Office Hours: Approximately one hour before and after class, generally by appointment. Other times can be arranged. Individual instructors will disseminate personal contact information.

## 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 will be helpful.

## Learning Objectives

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;
- U.S. 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.

Please note that 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. Similarly, though we will spend a good deal of time on how the United States has chosen to respond to the cyber situation to date, we will also explore alternative ideas and structures, since it is by no means clear that what we're doing as a nation today is the best possible course of action. You will be asked to read a number of current policy documents and related materials. In the end, you'll be asked to put these ideas together as they're applied today, as well as how they might be changed in the future. Hence, we will be exploring these new and exciting areas together.

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

## Course Policies

### Grading

An in-class test will be given at six weeks, plus an in-class final exam. All exams are cumulative.

Weighting 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*** due 29 October 2019 (thesis statement due 22 October) and
    - ***Assignment 3*** due 26 November 2019
- Simulation/Briefings: 15%
- Class Participation: 15%

Simulations and Briefings: These scenario-based exercises will be an opportunity for you to put into practice what you've learned in theory. They will be conducted several times during the term, with one involving a national-level scenario and others focused on a more military/operational scenario. In preparation for the early December exercise, you'll be asked to prepare a short paper (***Assignment 2***) and a proposed course of action (***Assignment 3***) to help prepare you for your role in the simulation (SEE appendices 2-3 for more details). Your Simulation/Briefing grade will be based on any verbal in-class presentation you give on your written assignments (especially ***Assignments 2 and 3***) and your contributions to group efforts during the exercise(s).

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. She will contact the instructor staff and provide directions to the section lead.

Course Conduct

- All requirements for the course (e.g., tests, projects, participation, etc.) must be completed for you to complete the course successfully.
- No papers or other materials that have been used for other courses may be used for this course.
- **Assignments are due no later than the announced due date.** Assignments submitted after this date will receive no credit unless prior arrangements have been made with the Professor.

- You must be present on the day you and/or your group have been assigned to participate in a simulation or make an in-class presentation. If not, you 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. Do not fall into this trap for any reason. Please see the materials at the Nimitz Library website (http://libguides.usna.edu/plagiarism) for further explanation. You 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) Don't modify, delete, or otherwise change the course readings, which will be in the same folder. If you want to have a copy of a document to annotate yourself or for some other reason, COPY IT from the file onto your 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 your understanding of cyber issues that affect your professional and personal lives.
(4) Read for context, synthesis, and as a basis for in-class discussion, not details.

**Course Outline**

A Note on Course Materials: In general, you will find the reading materials for this course in several places.

- Current periodicals, policies, and papers. This collection of reading materials has been uploaded to a shared folder and is available on the course web site. Assigned readings are keyed to topics in the syllabus.
    - ***Required*** readings are testable and will be the subject of classroom discussion.
    - ***Supplemental*** readings are intended to complement classroom discussion and to serve as a foundation for further research and study (especially for your individual effort writing assignments 1, 2, and 3)

- Books recommended for further reading (for background reading and your professional library):
    - 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

A Note on Dates: Dates for specific topics may change depending on the pace of learning and the availability of guest speakers. Your Professor will alert you to upcoming changes.

## Course Outline

**Tuesday, 20 August 2019: Course Introduction and "Big Ideas"**

- Defining "National Security Decision Making in the Cyber Age"
- Concepts of Power, Governance, Roles of the State and Individuals
- The benefits and drawbacks of an interconnected world
    - The nature of cyberspace and how it can be disrupted
    - US dependence on networks and data flows – contributions to economic growth, integration, and policy goals (e.g., democratization)
    - Implications for the US military -- the networked joint force in an interconnected world.
    - Contributions of cyber power to U.S. military operations
    - Focus areas for you as a Junior and Senior Officer

Readings:

[Required]

1. Review the Course Policy and Syllabus;
2. Review the preamble and first 10 amendments of the US Constitution;
3. "An Interview with General Paul M. Nakasone, Commander US Cyber Command", Joint Force Quarterly 92, January 2019
4. Review book summary: The Great Convergence – Information technology and the New Globalization, Richard Baldwin, Geneva Institute, 15 November 2016 (Optional video provided on SY403 site as well)
5. Inglis, "Cyberspace—Making Sense of it All";

[Supplemental]

1. Review the Slides on "Major Events in Cyberspace: What We Learned and What We Should Have Learned"
2. Surviving on a Diet of Poisoned Fruit – Reducing the National Security Risks of America's Cyber Dependencies, Richard Danzig, Center for A New American Security, 2014
3. Rubicon [Moment], Dan Geer, Stanford University Press, 2018
4. Cyber War and Its Strategic Context, Paul Bracken, Yale University, August 2017
5. "The Internet of Things in Action", The NextWeb 19 May 2013;
6. "The Future of Things Cyber", Strategic Studies Quarterly Spring 2011, Michael Hayden;
7. "Beyond Data Breaches – Global Interconnections of Cyber Risk", Zurich Cyber Risk, April 2014;
8. VIDEO: Cybersecurity and American Power, Gen. Keith Alexander, Commander, USCYBERCOM, AEI Talk, 9 July 2012

(http://www.aei.org/events/2012/07/09/cybersecurity-and-american-power/?roi=echo3-12517029639-9106864-4ec87e2d5b7fab7f3d88d9dd3d7d1b50&);

9. "Nearly every U.S. arms program found vulnerable to cyber attacks", Reuters 21 Jan 2015

**Thursday, 22 August 2019: Cyber Power Fundamentals**

- Who owns and runs cyber space?
- Cyber as a separate warfighting domain and/or in support of other domains
- Cyber Security – what is possible and what's not
- Concepts and definitions: offense, defense, deterrence, crime, espionage, sabotage
- Attributes of cyberspace that affect policy and military applications
    - Attribution problems, asymmetry, effects of cyber actions, public/private interfaces, privacy concerns

Readings:

[Required]

1. Commander US CYBERCOM Vision Statement, "A Cyber Force for Persistent Operations", Joint Force Quarterly 92, January 2019
2. *Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command* (Released 23 March 2018)
3. FACT SHEET: National Security Strategy 18 December 2017
4. "The Digital Vigilantes Who Hack Back", Nicholas Schmidle, NewYorker, 7 May 2018
5. FACT SHEET: DHS Cybersecurity Strategy 15 May 2018
6. "Defending a New Domain", William Lynn, Foreign Affairs, Sept/Oct 2010
7. Read cyber related portions (the yellow highlighted sections) of the 2019 National Defense Authorization Act (NDAA), Passed 4 August 2018, Signed into law on 13 August 2018
8. "Learn cyber conflict history, or prepare to repeat it", Jason Healey, Armed Forces Journal, November 2013

[Supplemental]

1. White House Policy on Cyber Deterrence, December 2015

**Tuesday, 27 August 2019: Threats and Vulnerabilities**

- Nature and dimensions of the threats to the interconnected world
    - Criminal, economic, critical infrastructure, intelligence, military
    - State and Non-State actors
    - The multi-polar nature of the threat: near peers vs. criminals and hackers

Readings:

**[Required]**

1. "The untold story of NOTPETYA, the most devastating cyberattack in history", Andy Greenburg, Wired Magazine, September 2019
2. Director of National Intelligence, Worldwide Threat Testimony to Senate Select Committee on Intelligence (pages 5-7), 29 January 2019
3. "Report on Foreign Economic Espionage in Cyberspace", U.S. National Counterintelligence and Security Center, 2018
4. "Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power", Chatham House, Keir Giles, Senior Consulting Fellow, Russia and Eurasia Programme, 21 March 2016
5. "Putin is Waging Information Warfare. Here's how to fight back", Mark Galeotti, NYT, 14 December 2106
6. SKIM: "The Cost of Malicious Cyber Activity to the U.S. Economy, US Council of Economic Advisors, February 2018
7. SKIM: Finite State "Report on Supply Chain Assessment Regarding Huawei Technologies Co., Ltd.", 2019
8. SKIM: U.S. Senate Select Committee Report on Russian Hacking of the 2016 Election, VOL I, 2019</FONT></b></a></li>Slides to Guide Discussion

**[Supplemental]**

1. "How Silicon Valley Became a Den of Spies", Zach Dorfman, Politico Magazine, 27 July 2018
2. Solar Sunrise: Dawn of a New Threat - 18 minute FBI Video from 1999 that eerily foretells the future
3. "Hack of the Democratic National Committee", Front Lines, 15 June 2016, Dmitri Alperovitch
4. "Russian Cyber War Possibilities WRT NATO", Riley and Robertson, Bloomberg News, 14 October 2015
5. "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies", Jordan Robertson & Michael Riley, Bloomberg, October 4, 2018
6. American Foreign Policy Council Defense Dossier (skim chapters on Russia and Iran), August 2012
7. "With Spy Charges, U.S. Draws a Line That Few Others Recognize", NYT 19 May 2014;
8. Hunting for Syrian Hackers' Chain of Command", NYT, 17 May 2013;
9. "Key Weapons Designs hacked", WaPo 28 May 2013;
10. "U.S. Oil and Gas at Greater Risk for Cyber Attacks", Fox Business 26 June 2013;
11. "Warring State - China's Cybersecurity Strategy" Center for a New American Security, Dec 2014;
12. "Cyber Threat and Response - Combating Advanced Attacks and Cyber Espionage", James Lewis, CSIS, March 2014;
13. 3 Simple Case Studies (Powerpoint slides) - Estonia, RSA/Lockheed, World Banking;

14. "China and Russia are using hacked data to target U.S. spies", LA Times, 31 August 2015;
15. "U.S. shadows Russian ship near nuke submarine bases", Bill Gertz, Washington Free Beacon, Washington Times, 4 September 2015
16. "Lessons from the Sony Hack", CryptoGram, Bruce Schneier, 15 Jan 2015

**Thursday, 29 August 2019: Combining Technology and Policy – a quick exercise (Exercise 1)**

- Expedited cyber exercise – "A Crisis Amongst the Internet of Things"
    - Diagnosing, Parsing, and Addressing Cyber Threats in a Massively Converged World

Readings:

[Required]

1. Exercise Background;
2. A model for Deterrence, Inglis
3. Notes for a model on deterrence, Inglis
4. White House Policy on Cyber Deterrence (December 2015)
5. SKIM: Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command (Released 23 March 2018)
6. SKIM: DoD Defense Science Board Cyber Deterrence Report (February 2017)

**Tuesday, 3 September 2019: USNA will follow a Monday Schedule (NO SY403 Class)**

**Thursday, 5 September 2019: Cyber Policy Evolution – Lesson 1 of 2**

- Evolution of cyber-related policies over multiple administrations
    - Critical infrastructure protection roots (Reagan)
    - Bush and Clinton approaches
    - Obama Administration
    - Trump Administration
    - DoD Cyber strategies
    - Congressional activities

Readings:

[Required]

1. White House Executive Order on Cyber Security, 11 May 2017
2. Chapter 1 of *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age*, Adam Segal
3. SKIM: Chapter 1: *The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War*, Steve Grobman and Allison Cerra
4. Review Chart depicting "Agreed Upon Roles Between DHS, DoD, and DOJ/FBI" (2010-2013)

5. PPD41, US Cyber Security Incident Coordination, 26 July 2016
6. Read cyber related portions (the yellow highlighted sections) of the 2019 National Defense Authorization Act (NDAA), Passed 4 August 2018, Signed into law on 13 August 2018
7. Remarks by Vice President Pence at the DHS Cybersecurity Summit, NYC, NY, 31 July 2018

[Supplemental]

1. Review list of major US cyber policy documents (note the rapid evolution over time…)
2. Evolving US Cybersecurity Policy: A Multi-stakeholder Approach, Henry M. Jackson School of International Studies University of Washington, Seattle Task Force Report Winter 2016
3. Commander USCYBERCOM Vision for Cyber Operations (2015)
4. Improving Critical Infrastructure Cybersecurity - PPD 21 (EO 13636) (PRECIS)
5. Administration Efforts on Cybersecurity: "The Year in Review and Looking Forward to 2016, White House, 2 February 2016"
6. Information Assurance (IA) Policy Chart;
7. The White House Blog 6 August 2013
8. PPD20 Government Fact Sheet (Full version remains classified)
9. PPD20 Insights, The Guardian, 7 June 2013;
10. (SROE) Defense News 27 May 2013;
11. Pentagon Is Updating Conflict Rules in Cyberspace, NYT 27 June 2013;
12. U.S. officials say NSA leaks may hamper cyber policy debate, Reuters, 7 August 2013;
13. CSIS Commission on Cyber Security 2011 update;
14. Policy History (Inglis) - Powerpoint Overview

**Tuesday, 10 September 2019: In Class Exercise - Ransomware**

Read exercise prep document

**Thursday, 12 September 2019: Cyber Policy Evolution – Lesson 2 of 2**

**Tuesday, 17 September 2019: Cyber Exercise 2**

**Thursday, 19 September 2019: Library Research Tutorial**

- Nimitz Hall room 108 – instructor will be Manuel Jusino (410.293.6925)
- Section 1201 will meet from 0830-0945 hrs
- Sections 3401 and 5601 will meet at regularly scheduled times
- Further details to be provided by Instructor

**Tuesday, 24 September 2019: Six Week Test (Grades due 1 October 2019)**

- Up through Cyber Policy Evolution

**Thursday, 26 September 2019: US Government Organization and Decision-Making Processes for Cyber Activities – Lesson 1 of 2**

- Current US government partition of responsibilities for cyber activities
  - Title 10 and Title 50 (and other) authorities
  - DoD organizations (USCyberCom, Service Components)
  - Intelligence Community
  - DHS and rest of Government
  - Congressional considerations

  Readings:

  [Required – Fear not, these will be adjusted as the semester proceeds]

  1. SecDef Memo Establishing US Cyber Command, 23 Jun 2009;
  2. Roadmap for Defending the Nation in Cyberspace: Key DOD Tasks, Paper for the Office of the Secretary of Defense, former Commander USCYBERCOM, June 2018
  3. Executive Order for Cyber, 11 May 2017
  4. The Presidents National Infrastructure Advisory Council Report on Securing Cyber Assets - Addressing Urgent Threats to Critical Infrastructure (August 2017)
  5. FACT SHEET: National Security Strategy 18 December 2017
  6. US National Security Strategy 18 December 2017
  7. USCYBERCOM Cyberspace Strategy Symposium Proceedings February 2018
  8. FACT SHEET (Congressional Research Service): on the 2018 National Defense Strategy Summary (Released 19 January 2018)
  9. 2018 National Defense Strategy Summary (Released 19 January 2018)
  10. Achieve and Maintain Cyberspace Superiority - Command Vision for US Cyber Command (Released 23 March 2018)
  11. FACT SHEET: DHS Cybersecurity Strategy 15 May 2018
  12. *DHS Cybersecurity Strategy (Full Version) 15 May 2018*
  13. Cyber Authorities Table
  14. FBI's Organization for Cyber - Cyber Norms, Initiatives, and Strategy (Comey, October 2015)
  15. PPD41, "U.S. Cyber Incident Coordination", 26 July 2016
  16. Function and internals overview of the National Security Council
  17. White House National Security Council Cybersecurity Tab

  [Supplemental]

1. Department of Defense role in protecting democratic elections - Testimony of Professor Richard J. Harknett before the Senate Armed Services Committee, 13 February 2018
2. [Is it] Time for a Separate Cyber Force?, ADM Jim Stavridis, USN (ret), Proceedings, January 2014
3. [DRAFT] National Defense Authorization Act Provisions for DoD Cyber (As of 27 November 2018)
4. John Hay Initiative Backgrounder - Demystifying Executive Order 12333, June 2016
5. Agreed Upon Roles Between DHS, DoD, and DOJ/FBI (2010-2013)
6. Commander USCYBERCOM Vision for Cyber Operations (2015)
7. Cyber Warfare and Cyber Terrorism, CRS Reports, 27 Mar 2015
8. National Security Strategy 2015
9. NextGov: Why Cybersecurity Dollars Don't Add Up, 30 Mar 2015
10. OMB Guidance for Cyber Strategy and Implementation Plan, 30 October 2015
11. Cyber Operations in DoD Plans, CRS Reports, 5 Jan 2015
12. NSA Cybercom Organizations, Schneier, 15 March 2014
13. NSA Chief: Military Not Organized for Cyber Warfare, National Defense Magazine, 12 June 2014
14. DoD Homeland Defense Strategy Feb 2013
15. Resilient Military Systems and the Advanced Cyber Threat, Defense Science Board, January 2013 (Exec Summary only)
16. Wall, Demystifying the Title 10-Title 50 Debate, 2011
17. DHS Blueprint Nov 2011 ExSumm, pp. 1-12; skim Appendix A
18. CRS Report on UCP and CoComs, 7 Nov 2011 (through page 15)
19. Dual-leadership role at NSA and CyberCommand stirs debate, WaPo, 6 Oct 2013
20. NRC 2009 Chapter 3 (sections 3.1 and 3.6, box 3.2; skim the rest)
21. 2007: NSPD-54/HSPD-23 aka, the CNCI (EPIC FOIA)
22. Clarke, Chapter 2, pp. 33-47
23. Singer pp. 133-139

**Tuesday, 1 October 2019: Guest Lecturer 2 – Niloofar Howe**

- An investor, executive and entrepreneur in the technology industry for the past 25 years, with a focus on cybersecurity for the past ten.
- Former chief strategy officer and senior vice president of strategy and operations at RSA, a global cybersecurity company where she led corporate strategy, corporate development and planning, business development, global program management, business operations, security operations, and federal business development

**Thursday, 3 October 2019: US Government Organization and Decision Making Processes for Cyber (Lesson 2 of 2)**

**Tuesday, 8 October 2019: Guest Lecturer Bill Ryder, Former NSA Senior Executive and Subject Matter Expert in Operations Research**

- "Zero day economics": Modeling the alignment of privacy and security

**Thursday, 10 October 2018: National and International Norms – lesson 1 of 2**

- Application of national and international norms to cyber power
    - Law of Armed Conflict
    - War Powers and Posse Comitatus
- Should these be changed in the face of cyber conflict?

Readings:

[Required]

**Russia:**

1. Russia's Approach to Information Warfare ***(skim),*** Michael Connell and Sarah Vogler, CNA, March 2017
2. The Gerasimov Doctrine, Politico.com, Molly McKew, September/October 2017
3. Assessing Russian Activities and Intentions in Recent US Elections, US Intelligence Community Report, January 2017
4. APT28: At the Center of the Storm Russia Strategically Evolves its Cyber Operations, FireEye, January 2017
5. Russia Blamed by Germany for Meddling, Tara Seals, InfoSecurity, 16 May2016

**China:**

1. China's Strategic Thinking on Building Power in Cyberspace, Triolo and Webster, New America ***(Skim)***
2. China's National Cyberspace Security Strategy, 27 December 2016
3. China's International Strategy of Cooperation on Cyberspace, March 2017
4. China's Cybersecurity Law (KPMG Overview), 7 November 2016
5. Mandiant Report on APT1 -- Exposing One of China's Cyber Espionage Units, February 2013 (Read Executive Summary and skim the rest)
6. Hiding I Plain Sight: FIREEYE and MICROSOFT expose obfuscation tactic, May 2015

**North Korea:**

7. North Korea's Cyber Capabilities: Deterrence and Stability in a Changing Strategic Environment, Foreign Affairs 12 September 2014
8. The World Once Laughed at North Korean Cyberpower, Sanger et al, NYT, 15 October 2017
9. Russia Provides New Internet Connection to North Korea, Foreign Affairs 1 October 2017

**Nominal Allies:**

10. UK: National Cyber Security Strategy 2016 to 2021 (skim)
11. UK: National Cyber Science and Technology Strategy, 2017
12. Israel: Review notes from Eviatar Mantania Guest lecture (12 September 2017)

**Regarding Norms:**

1. U.S. State Department Declaration of Norms (see page 8-9) - 14 May 2015
2. Fact Sheet: Tallinn Manual 1.0 (From NATO Cooperative Cyber Defence Centre of Excellence website)
3. Fact Sheet: Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (From NATO Cooperative Cyber Defence Centre of Excellence website)
4. What Tallinn Manual 2.0 Teaches Us About The New Cyber Order, Kalev Leetaru , Forbes.com, 9 February 2017
5. Singer, pp. 122-126;
6. Foreign Policy: Legality of Military Patrolling in Cyberspace, 5 Dec 2012
7. Schmitt: The Law of Cyber Targeting, Naval War College Review, Spring 2015
8. Law of Armed Conflict (LOAC) (Summary), Powers;
9. What Europe Got Wrong About NSA, Foreign Affairs Magazine, Flournoy and Klein, 2 August 2016
10. Safe Harbor 2 – A view from Schremms, Arstechnia, 2 Feb 2016, Jennifer Baker
11. DoD Cyberspace Policy Report Nov 2011;
12. Foreign Policy: Legality of Military Patrolling in Cyber, 5 Dec 2012;
13. Washington Post: Cyber Attack as an Act of War, 26 Oct 2012;
14. The Atlantic : Is it Possible to Wage a Just Cyberwar?, 5 June 2012;
15. Net Politics, “China’s Views on Int’l. Law” 29 Oct 2014;

[Supplemental]

1. Russian Hackers Stole NSA Spy Secrets, WSJ, 6 October 2017
2. Russia hacking more ... China less, 12 October 2016, Ken Dilanian, NBC News
3. American Bar Association Report, Jan 2010 (Chapter 3);
4. National Research Council report on Cyber Capabilities 2009, pp. 239-272;
5. CRS Report 15 Nov 2001 (ExSumm and pp. 1-6);
6. The Myth of Posse Comitatus, October 2000;
7. ABA Journal “What is the Role of Lawyers in Cyberspace?”, 1 May 2012;
8. Tallin Manual Draft 2013;
9. Schlanger, “Intelligence Legalism…” HNSJ, Vol. 6 2015
10. Cyberthreat Posed by China and Iran Confounds White House New York Times; Sanger, Sep 15, 2015
11. Court of Justice of the European Union, Safe Harbor Ruling - October 2015

12. Court of Justice of the European Union, Safe Harbor Press Release - October 2015

***Tuesday, 15 October 2019 – Assignment 1 due before class***

**Tuesday, 15 October 2019: Guest Lecturer, Tony Sharp, FedEx Chief Information Security Officer**

- Read (before class) the FedEx Strategy document on "Defense of a Global Enterprise"
- Research the *notPetya* attack on FedEx experienced in June 2017 as a basis for classroom discussion.

**Thursday, 17 October 2019: National and International Norms – lesson 2 of 2**

***Tuesday, 22 October 2019: Thesis Statement due for Assignment 2 (see appendix 2 for details)***

**Tuesday, 22 October 2019: Public Policy Issues in Cyber Space**

- Public policy issues
  - Public/private interfaces
  - Privacy
  - Alternative Views on how to set the "balance"
  - Ethical Considerations

Readings:
[Required]

1. "Apple and Other Tech Companies Tangle With U.S.", NYT, 8 Sep 2015
2. US Deputy Attorney General Rod Rosenstein prepared remarks about encryption on Tuesday, 10 October 2017, at the U.S. Naval Academy
3. Berkman Center Report, February 2016 "Don't Panic - Making Progress on Going Dark Debate"
4. Obstructing Governance by Consent, Eatinger, TheCipherBrief.com, 30 October 2016
5. US Surveillance Law, Safe Harbor, and Reforms Since 2013. Peter Swire, 17 December 2015
6. Policy frameworks for balancing individual and collective security in cyberspace: Statement of Chris Inglis before the Senate Armed Services Committee, 14 July 2016
7. "Cyberwar: More hype than reality", Foreign Policy March/April 2012;
8. WSJ: Should we let the Private Sector Hack Back?, 10 May 2015

[Supplemental]

1. US Surveillance Law from 1978 to 2004, Peter Swire
2. Internet Security Alliance Testimony June 2011;
3. Alternative Views: Overview: CSIS Commission on Cyber Security, 2011 Update, read pp 1-5, skim rest;
4. "Hyped Threat?": National Journal 23 July 2011;
5. A Legal Framework for Cyber Ops: Harvard (Steven Bradbury) Jan 2010
6. Klayman versus Obama, US District Court Opinion of the District of Columbia, November 2015
7. UK Investigatory Powers Bill (IPB), Summary of Draft, 2016
8. US Securities and Exchange Commission 13 Oct 2011;
9. Former Director CIA and NSA GEN Hayden urges authority to monitor networks, Wired Magazine 4 Oct 2011;
10. NRC 2009 Section 5.2;
11. 10 Conservative Principles for Cybersecurity Policy: Heritage Foundation Paper 10 Jan 2011 (esp. page 6-9);
12. Reason.com Sep-Oct 2011 ("Feds erect a bureaucracy to combat a questionable threat");
13. Constitution Project on Cybersecurity Policy;
14. Cyber and Civil Liberties: Huffington Post 22 Oct 2012;
15. CSIS "Cyber Threat Information Sharing – Recommendations for Congress" 10 Mar 2015
16. Ethics of Cyber War: Rowe, International Journal of Cyber Ethics, Jan-Mar 2010;
17. WSJ (Hacking Back) 7 June 2013

**Thursday, 24 October 2019: Guest Lecturer –** CAPT Dave Bondura, USN (ret) Former Deputy Director USNA Cyber Center, current cyber researcher, Johns Hopkins University

***Tuesday, 29 October 2019: Completed Assignment Two Due (see Appendix 2 for further details)***

**Tuesday, 29 October 2019 and Thursday, 31 October 2019 (2 periods): Economic Issues and Incentives Related to Cyber Decision Making (Prof Martin Libicki, RAND and USNA Cyber Center)**

- Economic issues
    - Protection of intellectual property
    - Alignment of incentives and externalities
    - The Advanced Persistent Threat
        - Calculating the cost of cyber espionage to the national economy
        - Costs and benefits of alternative incentive-based approaches to increase cyber security

- Principles for optimizing cyber security investments (Gordon-Loeb)

Readings:

[Required]

1. Singer, pp. 55-60;
2. ONCIX 2011 Report (ExSumm + through page 11);
3. IP Commission Report, 22 May 2013 (Exec Summary);
4. McAfee-CSIS Report July 2013 (Introduction);
5. Daniel Geer, et al "CyberInsecurity: The Cost of Monopoly, How the Dominance of Microsoft's Products Poses a Risk to Security";
6. Ross Anderson, "Why Information Security is Hard: An Economic Perspective";
7. Reuters 10 May 2013; Anderson, et al "Measuring the Cost of Cybercrime";
8. Anderson and Tyler Moore, "The Economics of Information Security";
9. Anderson and Shailendra Fuloria, "Security Economics and Critical National Infrastructure";

[Supplemental]

10. Spafford, On Competitions and Competence 7 April 2013 (for fun)
11. Cybersecurity and Trade: National Policies, Global and Local Consequences, Allan A. Friedman, September 2013

***Tuesday, 5 November 2019: 12 Week Grades Due***

**Tuesday, 5 November 2019:** Guest Lecturer TBD

**Thursday, 7 November 2019: Tactical Considerations in the Application of Cyber Power**

- Case Studies
  - Examples: Estonia, Georgia, Ukraine, Syria, Operation Orchard, Stuxnet, Flame
- Cyber War and Kinetic War
- How Cyber capabilities fit into Major Warfighting concepts
  - Examples: Joint Operational Access Concept; Joint Concept for Access and Maneuver in the Global Commons (formerly AirSea Battle)

Readings:

[Required]

1. The Defense of Battle Position Duffer - Integrating Cyber in Tactical Military Operations, September 2016
2. "Cyber War, Cyber Conflict, and the Maritime Domain" – National War College Review (on Cyber War), Spring 2014;
3. "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units", Published December 22, 2016, Crowdstrike Updated 23 March 2017

4. Cyber Offensive Capabilities at the Operational Level - Center for Strategic and International Studies (CSIS), Sept. 2013;
5. Syria War Stirs New Debate 24 February 2014, NYT.com;
6. "Russia's Alleged December 2015 Attack on Syrian Power Grid", Dan Goodwin, Ars Technia, Jan 2016
7. White House Blog (Michael Daniel), Disclosing Cyber Vulnerabilities, 28 April 2014;
8. "Fix holes or exploit them?", Bruce Schneier, 19 May 2014;
9. Stuxnet! CBS News 4 March 2012;
10. "Meet Flame" - Wired 28 May 2012;
11. "Obama Orders Sped Up Wave Of Cyberattacks Against Iran" - NYT 1 June 2012;
12. JCS Pub 3-12 R - Cyber Space Operations (Read the Executive Summary), 5 Feb 2013

[Supplemental]

1. Libicki Chapter 3, 6 and 7 (esp. pp. 154-158);
2. USSTRATCOM Cyber Warfare Lexicon 5 Jan 2009;
3. "Stuxnet and the Future of Cyber War" – Survival, Feb-Mar 2011;
4. Navy Strategy for Achieving Information Dominance 2013-2017;
5. "Plan X for Cyber War" - Danger Room Blog (Wired Magazine) 21 August 2012;
6. Stuxnet and North Korea - Reuters 29 May 2015;
7. "Plan X" - Washington Post, 30 May 2012;
8. DoD Joint Operational Access Concept (JOAC), Jan 2012;
9. Center for Strategic and Budgetary Assessments (CSBA) Air Sea Battle Operational Concept;
10. "Operationalizing Cyber War ", Defense Daily 28 May 2014;
11. NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack - NYT 31 Aug 2014;
12. "Cyber as Blunt Force Trauma" - Politico, 16 Apr 2015;
13. "Tactical Cyber: How to Move Forward" - Metcalf and Barber, Small Wars Journal 14 Sep 2014
14. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities, NRC 2009, table 2.1 and Chapter 8

**12, 14, and 19 November 2019 (3 periods): In Class Presentations based on assignment Two**

**Thursday, 21 November 2019 and Tuesday, 26 November 2019 (2 Lessons): Strategic Considerations in the Application of Cyber Power**

- Effective application of cyber power on defense and offense
- Impact of Strategic cyber war on trade relations and economic activity
- Deterrence postures for cyber space
- Arms control potentials for cyber space

Readings:

[Required]

1. Cyber Executive Order, the White House, 11 May 2017
2. An Index to National Cyber Strategies Around the World , NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), (Review and flag as an enduring resource) Updated monthly.
3. An Oncoming Administration - Blueprint for the first 100 Days (November 2016), Video link
4. "A Strategy for The Global Fight Against Cyber Attacks", CipherBrief, Butler, Kramer, Lotriente, 26 October 2017
5. A model for Cyber Deterrence, Inglis, 2015
6. "Why Is Finland Able to Fend Off Putins Information War?", Standish, Politico.com, 1 March 2017
7. Libicki on Cyber Deterrence, Appendix C;
8. Nuclear Lessons for Cyber Security, Joe Nye - Winter 2011
9. USNI "Don't Draw the Red Line" Oct 2011;
10. DoD Cybersecurity Policy Report Nov 2011 (esp. questions 1-5);
11. Cavaiola, Gompert and Libicki, "Cyber House Rules" 5 Feb 2015;
12. Gompert and Libicki, "Cyber Warfare and Sino-American Crisis Instability" 25 Jul 2014;
13. JCS Capstone Concept for Joint Operations 10 Sept 2012;
14. Joint Concept for Entry Operations, April 2014;
15. BPC Cybersecurity of Electric Grid, February 2014;
16. National Institute of Standards and Technology (NIST) Critical Infrastructure Cybersecurity Framework, February 12, 2014

[Supplemental]

17. A Presentation to Chinese Government Officials on US Cyber Strategy circa 2017 (Inglis: Shanghai Track 1.5 discussions, 29 November - 2 December 2017)
18. "Enemy without Borders", US Naval Institute, Oct 2012 [Supplemental]
19. 2016 U.S. National [Cyber] Action Plan
20. 2015 U.S. [Cyber] Strategy and Implementation Plan for Civilian Departments/Agencies
21. 2015 Executive Order Promoting Private Sector Cybersecurity Information Sharing
22. "Regulate cybersecurity or expect a disaster, experts warn Congress", CNN.com, Pagliery, 16 November 2016
23. Clarke, Chapters 6 and 7;
24. Gompert and Saunders, skim Chapter 6;
25. National Research Council Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber Attack Capabilities (2009) sections 9.1 and 9.2;
26. US DoD Joint Concept for Entry Operations, April 2014

***Note: Assignment 3 is due on 26 November 2019***

*Thursday, 28 November 2019: Thanksgiving (No class)*

**Tuesday/Thursday, 3 and 5 December 2019 (2 Periods): Graded Simulation Exercise**

Readings:

[Required]

1. Exercise Overview
2. Five Pacific Scenarios, Defense News, 24 Sept 12

[Supplemental]

1. Foreign Policy and Christian Science Monitor Articles 28 Feb 13
2. Study on Chinese Signaling April 2013, National Defense University
3. Congressional Research Service Report on Chinese Maritime Disputes R42784-2
4. China's Little Blue Men (China's proxies), Defense News, 9 Nov 2015
5. China Cyberwar Drill, The Atlantic Wire, 29 May 2013

**Tuesday, 10 December 2019: Finals Begin**

## Appendix 1: Assignment One

## SY403 - National Security Decision Making in the Cyber Age (Fall 2019)
## "Assignment One"

### Note the Deadline of 15 October 2019

**Assignment: Write a 5-7 page review and critique of <u>one</u> of the following books:**

- 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
- 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 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
- Wittes, Benjamin and Blum, Gabriella ***The Future of Violence***, New York, Basic Books, 2015

Each of the books cited above attempts to provide the reader with a summary of the history and a framework for understanding the implications of the age of cyber. Your assignment is to read the book and provide both a summary of the author's main points and a critical analysis on the author's conclusions regarding strategic implications and likely future trends (relating to cyberspace and our dependence on, and actions in and through, what the DoD describes as a "fifth domain").

You should (must) comment in your review on what you thought the author got right and what you find unsupported by either the facts presented or those you have gleaned from your cyber studies to date.

**This is an individual effort assignment to be turned in at beginning of class on 15 October 201**

**Appendix 2**: Assignment Two

## SY403 - National Security Decision Making in the Cyber Age
## "Assignment Two"

**Note the Deadlines of 22 October 2019 and 29 October 2019**

**Background:**

The end of course exercise for SY403 will be based on a hypothetical scenario which postulates future tensions between the US and the Peoples Republic of China (PRC). While hypothetical, the exercise will be based on a realistic portrayal of expectations, relationships, and tensions that do exist in the realm of cyberspace and the western pacific region.

The planned exercise will include consideration of US military forces deployed to the region and those supporting cyber operations, the full range of US instruments of power (separate and apart from military capabilities), allied expectations and initiatives, and, of course, the expectations, aspirations, and actions of the PRC.

**Assignment (to be turned in at beginning of class on 29 October 2019):**

Write a short (5-7 pages) paper outlining some aspect of the cyber landscape and/or the US-PRC relationship that will inform the exercise players in our December end-of-course exercise. You must choose a topic relevant to cyber operations, policy, capabilities. Sample theses are:

- *Making the case and plotting a course for Cyber Collaboration – now - between the PRC and the US*
- *Confidence through strength – the case for a vigorous offensive capability in countering Chinese adventurism*
- *Bringing Cyber into the 21st Century – the case for integrated kinetic and cyber actions*
- *Preventing conflict in the western pacific – what the US should do now to signal intent and avoid conflict*

Emphasis should be placed on determining and exposing the "facts on the ground" *and* on analysis that will inform decision makers during the exercise.

Sample elements/issues needed to support your thesis will be:

- What are the perspectives of the prospective participants in any western pacific contingency (esp, as regards cyber)?
- What are the capabilities of US, allied, and PRC forces to conduct cyber operations and/or to sustain kinetic operations in the face of cyber attack?
- What is the relationship between the DoD and other instruments of national and private power that might be "in play" during a western pacific contingency?

**You must submit your chosen title and thesis statement by 22 October 2018 (via e-mail to your instructor or in writing at beginning of class…)**

**Appendix 3:** Assignment Three – Due 29 November 2019

**National Security Decision Making in the Cyber Age**

**SY403**

**Fall 2019**

**Assignment Three** – Due **BEFORE** Class on 26 November 2019

Situation: You're a junior plans officer assigned to the J6 (C3/Cyber) shop at US Indo-Pacific Command in Hawaii. Because of your extensive knowledge across both political/military affairs and cyber defense and offense – being a Naval Academy graduate and having taken SY403 – the J6 (a Navy one-star) has assigned you as the liaison to the INDOPACOM Combat Mission Team assigned by US CYBERCOM.

As part of your duties, the Admiral asks you to prepare a short briefing regarding (a) the unfolding situation over disputed islands in the East China Sea; and (b) Chinese views on use of cyber offensive capabilities for strategic and tactical purposes.

The dispute is between Japan and China, each claiming ownership over islands they call Senkaku and Diaoyu, respectively.

Assignment: You are to prepare an **annotated** PowerPoint briefing of no more than five slides … or a single sheet of Talking Point (bullets) covering the following material:

- Background and History of the Dispute
- Recent Developments, including potential spillover effects from recent South China Sea activities
- Chinese views on use of cyber offense
- How the PACOM cyber posture should change with increasing levels of world tension and US military alert posture, including the role of the PACOM Combat Mission Team

Be sure to cite your sources as you would in a research paper.

**Slide deck or TPs due NLT 1330 on 26 November 2019.**

In naming your file be sure to include your last name

Example: "Smith_AssignmentThree.docx" or "Smith_AssignmentThree.pptx"