

POLITICS OF CYBERSPACE

Course Description

M. E. Kabay, PhD, CISSP-ISSMP

Program Director, MSIA | School of Graduate Studies

Associate Professor of Information Assurance | School of Business & Management

1 Course Description

As computing and networking technologies increasingly pervade the worlds of business, government, science, law enforcement, the military and entertainment, political and policy considerations also increase in importance as the Internet reaches an ever-greater portion of humanity. Highly controversial subjects involving government actions, legal theory, ethical judgements, international relations, and economic analysis are introduced with reference not only to historical developments of the last several decades but also to recent news reports. The course assumes only a rudimentary familiarity with the basic concepts and terminology of modern Internet usage and computing and is not a technology-focused course. This course offers students from all majors the opportunity to explore policy issues in greater depth than in technology-oriented courses they may have taken. Information-technology courses are not a prerequisite and students from all majors are welcome.

Prerequisites: Open only to juniors and seniors. (3 Credits)

2 Course Objectives

By the end of this course, students will be able to present summaries and intelligent arguments about the facts, the issues, the players and the costs and benefits involved in key political debates about topics such as the following and others that develop through discussion in the course:

- Cyberspace and the new politics: moving on from face-to-face communication in politics; electronic voting; disintermediation of political speech
- Political control of the Internet including the Domain Name System
- Global patterns of Internet censorship: The Great Firewall of China and whether it and others like it can and ought to survive for long in the 21st century
- Internet neutrality: the issue of differential service and access imposed by Internet service providers
- The economics of software: who pays for bugs? What are the consequences of software monocultures?
- The full disclosure debate: whether vulnerabilities should be published quickly and openly or not
- The changing face of cybercrime: cybermercenaries, organized crime, and information warfare
- The intellectual property wars – the economics of intellectual property in a networked world: piracy of music, video, pictures, and text; digital rights management; reverse engineering; open-source software; wikis
- Virtual worlds: anonymity, pseudonymity, gaming, cybersex, cyberporn, social networking, griefers, cyberbullying, cyberstalking, addiction, and virtual economies
- Privacy in the digital world: public records online, search and seizure, warrantless wiretapping; changing conceptions of privacy across generations

- The psychology of risk: misconceptions, misinformation, and misjudgement; the information underpinnings of the War on Terror; cyberterrorism
- The cryptography wars: export regulations, legal status of memorized passphrases for decryption keys
- Code as speech: should writing malware be illegal?
- The digital divide: changing demographics of Internet access; educational and cultural effects of Internet- and computer-deprivation

3 Course Schedule & Location

- Tuesdays and Thursdays from 08:00 to 09:15 (75 minutes) in Dewey 108

4 Texts

- Lessig, L. (2006). *Code: And Other Laws of Cyberspace*, Version 2.0. Basic Books (ISBN 0-465-03914-6). 432 pp. \$12.89 (Amazon)
- Palfrey, J. & U. Gasser (2008). *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books (ISBN 0-465-00515-2). 288 pp. \$17.13 (Amazon)
- Acohido, B. & J. Swartz (2008). *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. Union Square Press (ISBN: 1-402-75695-X). 304 pp. \$13.57 (Amazon)
- Additional readings will be assigned during class and made available on the course Web site at < <http://www.mekabay.com/courses/academic/norwich/is406/index.htm> > or placed on reserve at the Kreitzberg Library.

5 Method of Assessment

- Research Report: 40%
 - Students will prepare a research report (5,000±1000 words / 10 single-spaced pages) focusing on specific aspects of the subject matter of the course.
 - Topics must be approved by the instructor by the indicated deadline (see Syllabus); duplicate topics are not authorized.
 - See the Term Paper Guidelines for detailed instructions.
- Presentation: 20%
 - Students must prepare a 30-minute presentation to the class on their research topic as part of the normal class schedule of the course.
 - The presentation schedule will be published in January after the topics are assigned through individual discussion with the instructor.
- Closed-Book Review Quizzes: 10%
 - Four announced *closed-book* quizzes testing key concepts from about two weeks of material are scheduled throughout the semester as shown on the syllabus.
 - The quizzes will consist of five short-answer questions to be completed in ten minutes.
 - Quizzes are intended to encourage review and to help prepare students for the mid-term exam and the final exam. They are not designed as onerous burdens on the students. There are no trick questions and short answers may be in point form rather than full sentences.
 - The schedule of the planned quizzes is in the class syllabus.
- Open-Book Midterm Exam: 10% **date**
 - 60-minute, open-book in-class exam covering the material to date.

- Materials permitted during open-book exams include only the assigned texts and student notes.
- Open-Book Final Exam: 20% **date and place**
 - Cumulative 2.5 hour, open-book final exam (see note in mid-term exam about materials permitted) administered during the official exam period.
- Optional extra-credit online discussions up to extra 10% of final grade
 - Every week, the instructor will pose questions to stimulate thought and discussion among members of the group
 - Students may also pose questions for discussion
 - Grading will follow the rubric distributed in the document about Online Discussions.

6 Notes

- There will be no *grading on a curve*. There are no predetermined numbers of final letter grades.
- Students are encouraged to study together but may not collaborate during exams. Students are individually responsible for all assigned readings, lecture, and discussion material, unless otherwise noted.
- In accordance with University regulations, students who miss more than three lectures without authorization or approval will be dropped from the course with an F grade. Students taking the Thursday class should note that each hour of the class counts as one lecture.

7 Cheating and Plagiarism

Students are graded on an individual basis and must therefore complete their own work. Students are reminded of the University's Policy against cheating and plagiarism which is available in the *Academic Rules & Regulations* < <http://www.norwich.edu/about/policy/academic/universityCatalog-academicRulesAndRegulations.pdf> > in "Appendix I – Academic Dishonesty." Paragraph 3 of that section reads as follows:

Plagiarism is the use of words, ideas, concepts, or work of another, without proper acknowledgment. The direct quotation of the words of another must be set off in quotation marks and acknowledged in a footnote or other acceptable form of citation. The use of paraphrased material, or the ideas, concepts, or work of another must also be acknowledged in a footnote or other acceptable form of citation. Acknowledging sources used in the preparation of an assignment solely in a bibliography does not constitute an acceptable acknowledgment of the words, ideas, concepts, or work of another used in the assignment. In any case where a student is found to have used plagiarized material, an academic penalty will be assessed.

Ignorance of the University's Rules is not a valid defense against accusations of academic dishonesty. If in doubt as to what constitutes plagiarism, ask before submitting assignments. Instances of cheating and of plagiarism will be reported to the Academic Integrity Committee. Penalties include expulsion from the University.

8 Contact Information

Professor Kabay (< mkabay@norwich.edu > or < mekabay@gmail.com >) is available at the School of Graduate Studies at 10 Depot Square in Northfield by appointment – which can consist simply of calling to see if he’s in and then coming to visit him.

Students are welcome to call him at **(802) 479-7937** at any time (that number follows him from home office to cell phone to University office and can never disturb him); if necessary, leave a voice-mail message with a return number.

To use instant messaging and video chats ask to be registered as buddies on these IDs (send e-mail to < mkabay@norwich.edu > or < mekabay@gmail.com >) with your IM service and ID) and then check the availability status:

- AIM: msiapd
- Yahoo: mich_kabay
- MSN: mekabay@gmail.com
- ICQ: 460817550
- Skype: mekabay

9 About your Instructor

M. E. Kabay began programming computers in assembly language in 1965. In 1976, he received his PhD from Dartmouth College in applied statistics and invertebrate zoology and taught biology, statistics and programming courses as a university professor in Canada and overseas. In 1979, he joined a compiler team for a new 4GL and RDBMS in the U.S. and then joined Hewlett-Packard Canada in 1980 as an operating systems and database performance specialist, winning the Systems Engineer of the Year Award in 1982. He earned his CISSP (Certified Information Systems Security Professional) designation in 1997. He served as Director of Education for the National Computer Security Association (NCSA, later ICSA and then TruSecure) from 1990 to 1999 and then worked with AtomicTangerine where he supported the International Institute for Information Integrity® (I-4®). Since 1986, he has published over 950 articles in operations management and security, written a college textbook on enterprise security (McGraw-Hill, 1996), and served as Technical Editor of the 4th Edition of the Computer Security Handbook (Wiley, 2002). He writes two security-management columns a week distributed by Network World and is working on the 5th Edition of the *Computer Security Handbook* which will be published in January 2009. He has been an invited lecturer at the United States War College, NATO HQ, and at NATO Counterintelligence training in Germany. He was inducted into the ISSA (Information Systems Security Association) Hall of Fame in December 2004 and earned his ISSMP (Information Systems Security Management Professional) designation in November 2005. Dr Kabay is Associate Professor of Information Assurance in the School of Business and Management at Norwich University, Northfield, VT 05663-1035 USA and currently the full-time Director of the Master's Program in Information Assurance in the School of Graduate Studies (SGS) where he is also the CTO (Chief Technical Officer) of the SGS. In Fall 2009 he will return to the School of Business & Management full time.

Web site < <http://www.mekabay.com> **Error! Hyperlink reference not valid.** >

Course Web page < <http://www.mekabay.com/courses/academic/norwich/is406b/index.htm> > or
< <http://tinyurl.com/57ebm2> >

Network World article archive < <http://www.networkworld.com/newsletters/sec/> >



10 Appendix: Tables of Contents

Palfrey, J. & U. Gasser (2008). *Born Digital: Understanding the First Generation of Digital Natives*. Basic Books (ISBN 0-465-00515-2). 288 pp. \$17.13 (Amazon)

1. Identities
2. Dossiers
3. Privacy
4. Safety
5. Creators
6. Pirates
7. Quality
8. Overload
9. Aggressors
10. Innovators
11. Learners
12. Activist
13. Synthesis

Acohido, B. & J. Swartz (2008). *Zero Day Threat: The Shocking Truth of How Banks and Credit Bureaus Help Cyber Crooks Steal Your Money and Identity*. Union Square Press (ISBN: 1-402-75695-X). 304 pp. \$13.57 (Amazon)

Prologue

Introduction

1. Built For Speed
2. System Simulation
3. System Fissures
4. Self-Anointed Adventure
5. The Convenience Quotient
6. Predators And Opportunists
7. Perpetuating Errors
8. Cost Of Doing Business
9. Vulgar Cheeks And Swindles
10. Hungry Sharks
11. Perception Challenge
12. Larger Rings
13. Public Acceptance
14. Gaps In The System
15. Keys To The Possible

16. Self-Contained Units

17. Under Siege

18. What Must Be Done

Epilogue

Appendix A Personal Security And Advocacy

Appendix B. Survey Of Security Experts

Glossary

Lessig, L. (2006). *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books (ISBN 0-465-03914-6). 432 pp. \$12.89 (Amazon)

INTRODUCTION

1. Code is law

2. Four puzzles from cyberspace

PART I: "REGULABILITY"

3. Is-ism: is the way it is the way it must be?

4. Architectures of control

5. Regulating code

PART II: REGULATION BY CODE

6. Cyberspaces

7. What things regulate

8. The limits in open code

PART III: LATENT AMBIGUITIES

9. Translation

10. Intellectual property

11. Privacy

12. Free speech

13. Interlude

PART IV: COMPETING SOVEREIGNS

14. Sovereignty

15. Competition among sovereigns

PART V: RESPONSES

16. The problems we face

17. Responses

18. What Declan doesn't get