

CJ341: Cyberlaw & Cybercrime

M. E. Kabay, PhD, CISSP-ISSMP

**Assoc Prof of Information Assurance
School of Business & Management, Norwich University**

Course Description

The computer has become a common tool in crime. This course examines the nature and scope of cybercrime and the legal response to high-tech crime, including the challenges presented to legal frameworks. The lectures and readings identify and discuss core cybercrime issues and the prevailing legal authorities (statutes, regulations, policies) that address these issues. The course also examines developing trends in cybercrime and cyberlaw. Students learn about the global nature of computer crime and examine national and international laws, regulations and agreements that govern computer crime, including computer investigations, prosecution and defense. The course encourages analytical thinking and reasoning about computer crime topics and relevant legal issues so that students can identify, analyze, and solve problems in the continually emerging cybercrime and cyberlaw issues and trends. The course explores legal responses to cybercrime, including regulatory and law enforcement initiatives aimed at combating computer crime. Prerequisites include basic courses in computing and in criminal law.

Prerequisites: IS120 or IS130 and CJ201 or permission of instructor. (3 Credits)

Course Objectives

By the end of this course, students will be able to

- Identify and discuss the key laws and issues that relate to cybercrime and cyberspace, including laws governing attacks and motivation of attackers;
- Label and describe different types of high-tech crime such as unauthorized access, denial of service, child pornography, auction fraud, on-line gambling, securities fraud, identity theft, cyberstalking, spam, and defamation;
- Classify and discuss at a management level crimes of intellectual property involving patents, trade secrets, copyright, fair use, digital rights management, trademarks and domain names;
- Define the international crimes and laws relevant for computer crimes;
- Determine the evidentiary value of computer-related devices and media;
- Describe how to seize, preserve, protect and transport computer-related evidence in accordance with legal statutes and official guidelines;
- Prepare for effective, professional testimony in court cases involving computer forensic evidence;
- Intelligently discuss legal and policy issues relating to government surveillance and warrantless searches.

Course Schedule & Location

- Thursdays 13:10:03 – 15:59:57 in Dewey 106

Texts

- Burgunder, L. (2008). *Legal Aspects of Managing Technology, Fourth Edition*. Thomson West Legal Studies in Business (ISBN 0-324-39973-1). xv + 683. Index.
- Moore, R. (2005). *Cybercrime: Investigating High-Technology Computer Crime*. Matthew Bender & Co. (ISBN 1-59345-303-5). xii + 258. Index.
- Clifford, R. D. (2006). *Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime, Second Edition*. Carolina Academic Press (ISBN 1-59460-150-X). xii + 282. Index.
- Additional readings will be assigned during class and made available on the course Web site at < <http://www.mekabay.com/courses/academic/norwich/cj341/> >.

Course Web Site

Course materials are posted at < <http://www.mekabay.com/courses/academic/norwich/cj341/> >

Methods of Assessment

- Research Report: 25% total
 - Students will prepare a research report (3,000-4,000 words / 6-8 single-spaced pages) dealing with legal, moral, educational, or other non-technical aspects of cybercrime, intellectual property law, or computer-mediated crime. Students must work with their instructor to select and refine a suitable topic.
 - See the *Term Paper Guidelines* document for full details. < <http://tinyurl.com/cj341-tpg> >
- Review Quizzes: 20%
 - Four announced *closed-book review* quizzes testing fundamental concepts from two or three weeks of material will be scheduled throughout the semester as shown on the syllabus.
 - The quizzes will consist of multiple-choice questions and short-answer questions to be completed in 10 minutes.
 - Quizzes are intended to encourage review and to help prepare students for the mid-term exam and the final exam and are not designed as onerous burdens on the students. There are no trick questions and written answers may be in point form rather than full sentences.
- Midterm Exam: 15% **THURSDAY 15 OCT 2009**
 - 45-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.
- Final Exam: 25%
 - Cumulative 2.5 hour, open-book final exam administered during the official exam period. Same general description as mid-term term
- Presentation: 15%
 - Students must prepare a ten-minute presentation on their report topic.
 - The presentation schedule will be published in September after the topics are assigned through individual discussion with the instructor.

- Online Discussions: up to 10% extra on final grade
 - Students may respond to discussion topics each week using the MOODLE classroom set up for the entire class starting in the second week of class.
 - See the *Online Discussion Guide* for details at < <http://tinyurl.com/cj341-old> >
- Extra Work:
 - Students may submit extra work for extra points on their final grade with permission of the instructor.
 - For example, the instructor will agree to accept suitable short essays such as summaries of interesting articles or books relevant to the course materials.
 - The rate granted for extra work is 1 point added to the final grade for 500 words of professional-grade writing. Thus a 1,000 word essay could improve the final grade by 2 points.
 - Particularly good book reports may be suitable for publication in *Network World* for even more credit.

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 < <http://www.norwich.edu/about/policy/academic/appendix1.html> >. 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.

Attendance Policy – no more than 1 unexcused absence

University regulations stipulate that “Unless stated otherwise, the maximum number of permitted absences is the number of times the course meets per week. When the student has reached the maximum number of permitted absences, the faculty member will warn the student of impending dismissal from class with a grade of ‘F.’ This warning letter will include the course number and section and dates(s) of absence(s). The letter will state that any future unexcused absences may result in recommendation to the Vice President of Academic Affairs through the course School Dean that the student be dismissed from the class with a grade of ‘F.’ A copy of the warning letter will go to the student’s academic advisor and to the Commandant and Vice President of Student Affairs.” (See pp 69-70 of the PDF version of the *Academic Regulations* available online at < <http://tinyurl.com/nuar2009> >.)

Additional Notes

- Students are expected to read the assigned readings before coming to class, discuss them in class, and then to review them after the class.
- There will be no *grading on a curve*. There are no predetermined numbers of final letter grades.
- Review questions will be distributed to students throughout the term. These example questions will not limit the scope of actual exam questions, and are merely intended for exam preparation.
- 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 (specifically, the case studies result in the same grade for each team member).

Office Hours & Contact Information:

Professor Kabay (<mailto:mkabay@norwich.edu>) is available in Dewey 209 any time his office door is open – feel free to walk in!

His office hours are posted on his door in Dewey 209 and on his Web site at

< http://www.mekabay.com/office_hours.htm > and

< http://www.mekabay.com/office_hours.pdf >.

Students are welcome to call him at (802) 479-7937 at any time (that number rings in his office or his cell phone but cannot disturb him); leave a voice-mail message with a return number if necessary.

Students may also use Instant Messaging at any time using

- Skype (by preference) at mekabay; other IDs are
- AIM: msiapd,
- Yahoo: mich_kabay,
- MSN: mekabay@gmail.com,
- Google: mekabay; or
- ICQ: 460817550 (on demand only)

About your Instructor: M. E. Kabay, PhD, CISSP-ISSMP

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 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 and teaching primarily MPE operating system, IMAGE/3000 database and VPLUS/3000 GUI-design courses as well as serving as support engineer to HP's hospital and university customers and managing HP's call center (*Phone-In Consulting Service*) for Québec & the Maritime provinces.

He served as Director of Education for the National Computer Security Association (NCSA, later ICSA and then TruSecure) from 1991 to 1999 and then worked with AtomicTangerine where he supported the International Institute for Information Integrity® (I-4®). He collaborated in the committees defining the *Common Body of Knowledge* for the Certified Information Systems Security Professional (CISSP) designation in the mid-1990s and earned his CISSP in 1997.

Since 1986 (and as of mid-2009), he has published over 1,000 articles in operations management and security, written a college textbook on enterprise security (McGraw-Hill, 1996), and served as Technical Editor of the 4th (2002) and 5th (2009) editions of the *Computer Security Handbook* (Wiley) in collaboration with Senior Editor Seymour Bosworth and (5th ed) Managing Editor Eric Whyne. He writes two security-management columns a week distributed by *Network World*.

He has been an invited lecturer at the United States War College, the Pentagon, NATO HQ in Brussels, and at NATO Counterintelligence training in Germany. He was inducted into the Information Systems Security Association (ISSA) *Hall of Fame* in December 2004 and earned his *Information Systems Security Management Professional* (ISSMP) designation in November 2005.

From 2002 to 2009, he was the Director of the *Master's Program in Information Assurance* (MSIA) in the School of Graduate Studies (SGS) at Norwich University, Northfield, Vermont where he was also the Chief Technical Officer of the SGS from 2007 to 2009. Since June 2001, Dr Kabay has been Associate Professor of Information Assurance in the School of Business and Management and was appointed Associate Chair of Computing and Program Director of the new Information Operations programs in July 2009.

