SOCHE
Southwestern Ohio Council for Higher Education

CEDARVILLE UNIVERSITY

Cybersecurity: Legal and Ethics

National Cybersecurity Curriculum Project

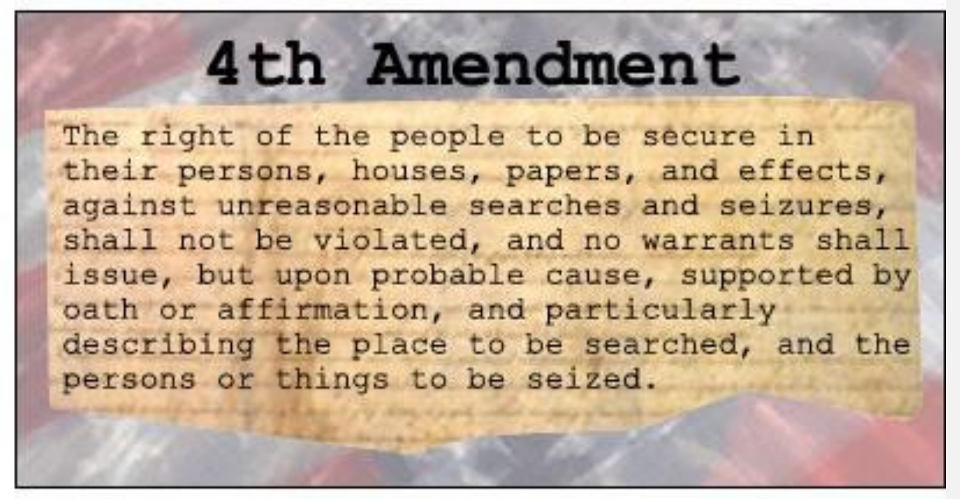
Seth Hamman, Ph.D., Sean Creighton, Ph.D.

Cybercrime

Computer Fraud and Abuse Act

- the language is broad, which makes it easy to apply but difficult to stick
- first conviction was Robert Tappan Morris' Internet worm
- does it make cyber bullying illegal?
- does it make beating casinos in computer poker by exploiting a programming bug illegal?

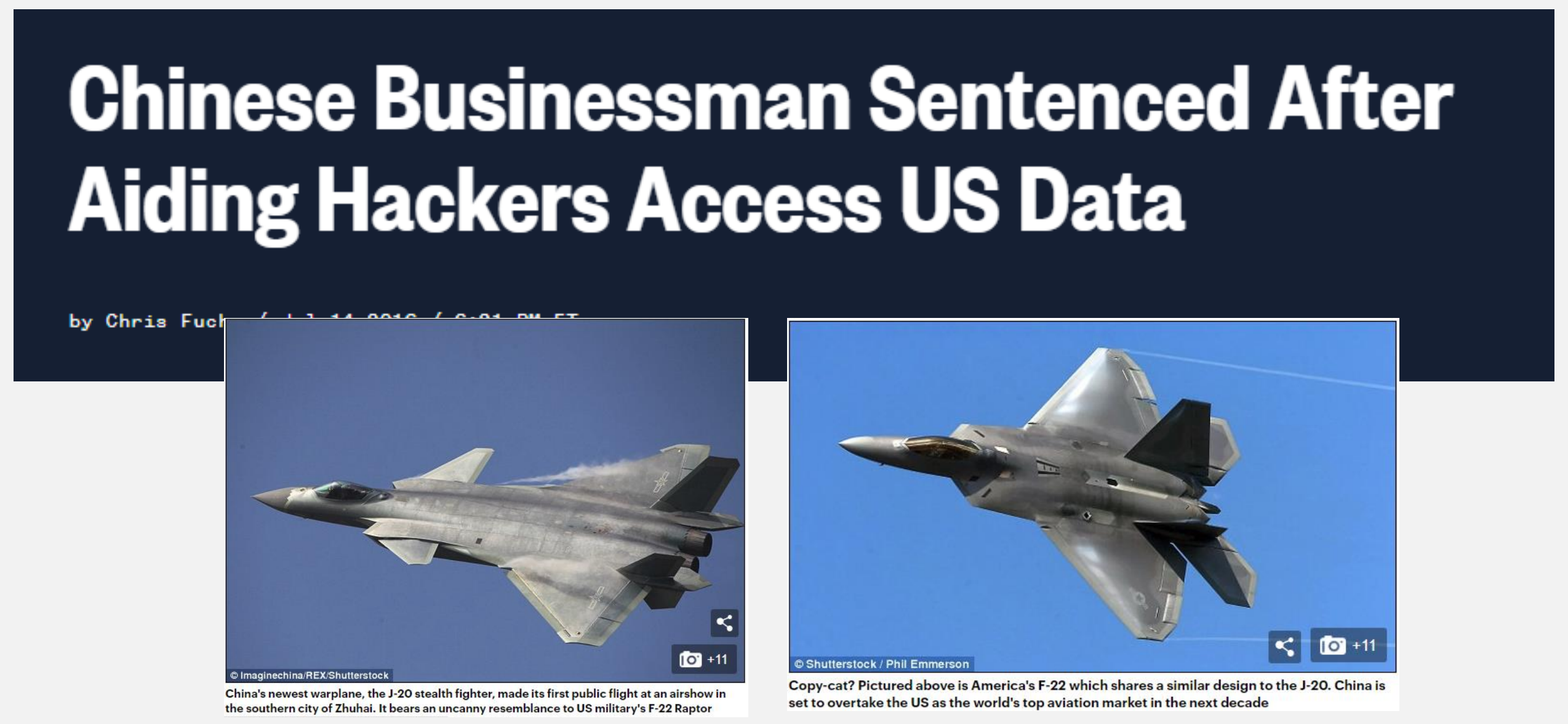
Electronic Communications Privacy Act


4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

- protects our 4th amendment rights to privacy, even in cyberspace
- all hinges on "reasonable expectation of privacy"
- is email, social media, work computer, etc. private?
- use of labels is important

Economic Espionage Acts


Chinese Businessman Sentenced After Aiding Hackers Access US Data

by Chris Fuch

© Imaginechina/REX/Shutterstock

China's newest warplane, the J-20 stealth fighter, made its first public flight at an airshow in the southern city of Zhuhai. It bears an uncanny resemblance to US military's F-22 Raptor

© Shutterstock / Phil Emmerson

Copy-cat? Pictured above is America's F-22 which shares a similar design to the J-20. China is set to overtake the US as the world's top aviation market in the next decade

The United States Constitution

Overview

This curricular module will be comprised of three micro-modules: one focusing on cybercrime, one on cyber warfare, and one on cyber ethics. Specifically, the curriculum will detail the differences between U.S. Code Title 10 (Armed Forces), Title 50 (War and National Defense), and Title 18 (Crimes); it will explain the relevant national cybersecurity legislation (e.g., the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, etc.); it will cover international law as it relates to cyber warfare (e.g., jus ad bellum and jus in bello); and it will provide multiple real-world examples of court cases and international cyber incidents that will engage students and encourage discussion. The module will be a stand-alone unit that can be "plugged in" to any college or university-level cybersecurity course, and will not require instructors to have any background in law.

Curriculum Package

3 Lessons of approximately 1 hour each

- Lesson 1: Cyber Ethics
- Lesson 2: Cybercrime
- Lesson 3: Cyber Warfare

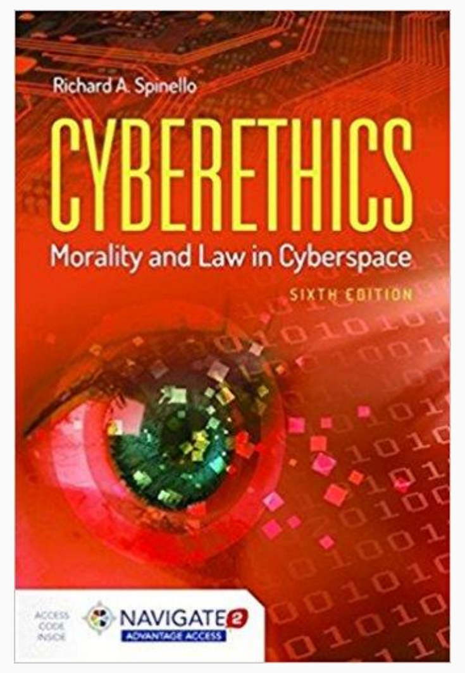
Materials

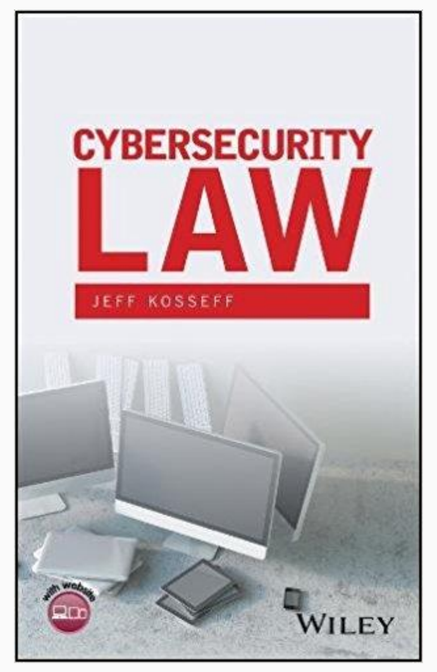
- PowerPoint Slides with extensive notes
- Assessment materials
- Custom videos and case studies

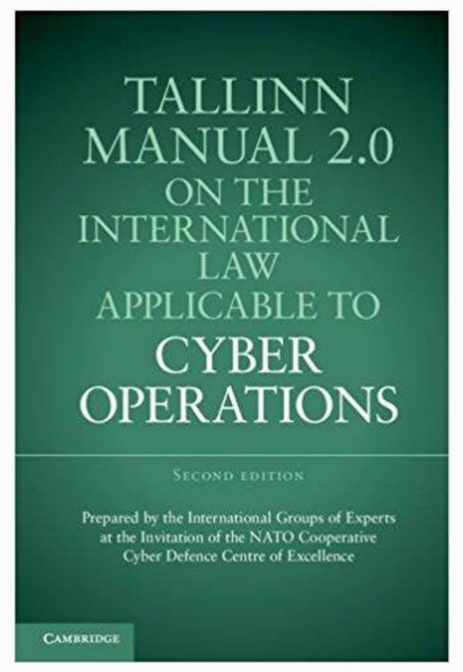
Case Studies

- **Game King Video Poker** – *is exploiting a software bug in a video poker machine a violation of CFAA? The motion to dismiss challenged the definitions of "protected computer," "without authorization," "exceeded his authorized access" (see left panel)*
- **Cyber Bullying Mom** – *the case of a mom whose cyber bullying led a teenager to kill herself, but did the mom do anything illegal? State laws were enacted after the fact – too late for this case*
- **Phone Phreakers (Kevin Mitnick)** – *early hackers who were more interested in accumulating trophies than making a living via cybercrime*
- **Robert Tappan Morris** – *first conviction of the CFAA, but judge was lenient because Morris did not fit the profile of a convicted criminal*
- **Aaron Swartz**– *sad case of a troubled young man charge with the CFAA*
- **Max Vision** – *a grey hat hacker who ran a major carding ring and was sentenced to 13 years in prison*
- **Sony Doxing Attack by North Korea** – *President Obama called this an act of "cybervandalism" but was it an act of war? What type of damage would have been necessary for it to qualify as such?*
- **Stuxnet** – *kinetic effects resulted from this cyber operation. Was this an act of war that could have provoked an armed conflict?*
- **Estonian Cyberattacks** – *Russian revenge on Estonia demonstrated the damage that cyber warfare could inflict on a country with a dependence on the Internet*

Recommended Reading


Richard A. Spinello
CYBERETHICS
Morality and Law in Cyberspace
SIXTH EDITION
NAVIGATE 2 ADVANTAGE ACCESS


CYBERSECURITY LAW
JEFF KOSSEFF
WILEY


TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS
SECOND EDITION
Prepared by the International Groups of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence
CAMBRIDGE

Cyber Warfare

Mission Statement – USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries.

- "Under the law governing the resort to force between states (**jus ad bellum**), it will have to be determined in what circumstances, if any, cyber operations can amount to (a) an internationally wrongful threat or use of 'force', (b) an 'armed attack' justifying the resort to necessary and proportionate force in self-defense, or (c) a 'threat to international peace and security' or 'breach of the peace' subject to UN Security Council intervention." *(from Melzer's "Cyberwarfare and International Law")*
- "Under the law of armed conflict (**jus in bello**), here referred to as international humanitarian law (IHL), 'cyberwarfare' must be distinguished from phenomena that are not necessarily governed by IHL, such as 'cyber criminality' and 'cyberterrorism'. Where IHL does apply, it must be clarified to what extent its rules and principles, designed to govern traditional means and methods of warfare, can be transposed to cyberwarfare. In doing so, the focus will be on the rules and principles of IHL governing the conduct of hostilities rather than those governing the protection and treatment of persons in the hands of a party to an armed conflict, which is an area less relevant for cyberwarfare." *(from Melzer's "Cyberwarfare and International Law")*
- Cyber attacks are restricted to military members of DoD, as restricted by international law. Authorities are derived from U.S. Code Title 10
- Title 50 covers intelligence and defensive operations, including covert operations such as spying and cyber espionage

Cyber Ethics

Student Outcomes

- "Students will be able to evaluate the relationship between ethics and law, describe civil disobedience and its relation to ethical hacking, describe criminal penalties related to unethical hacking, and apply the notion of Grey Areas to describing situations where law has not yet caught up to technological innovation." *(from NSA CAE-CO Academic Requirements, M.10)*
- "Students will be able to describe steps for carrying out ethical penetration testing, describe ethical hacking principles and conditions, distinguish between ethical and unethical hacking, and distinguish between nuisance hacking, activist hacking, criminal hacking, and acts of war." *(from NSA CAE-CO Academic Requirements, M.10)*