ECE 498KL: eCrime and Internet Service Abuse

Kirill Levchenko

October 25, 2018

ILLINOIS
Electrical & Computer Engineering
COLLEGE OF ENGINEERING

Instructor and TA

- **Instructor**: Kirill Levchenko
  - **Email:** `klevchen@illinois.edu`
  - **Office hours:** Mondays 2:00 PM in CSL 468
- **TA:** Joshua Reynolds
  - **Email:** `joshuar3@illinois.edu`
  - **Office hours:** Thursdays 1:00 PM in CSL 221

Time and Place

- **Lectures**
  - Tuesdays and Thursdays 2:00 PM to 3:20 PM
  - ECE Building room 2015
- **Final exam**
  - December 14 at 8AM
  - ECE Building room 2015

Web

- **Class site**
  - https://courses.engr.illinois.edu/ece498kl/fa2018
  - Readings assignments and machine problems will be posted here
- **Piazza site**
  - https://piazza.com/illinois/fall2018/ece498kl
  - Instructor and TA will monitor site and respond to comments
  - For urgent matters, contact instructor or TA directly

Class Goals

- Reason about computer systems being *abused* for profit
  - Need to think *adversarially*
  - You will learn to do this
- Know the state of the art in attacks and defenses
  - Not enough time to cover everything
    - You will have learn the rest as you need it in practice
  - Security evolves rapidly
    - You must keep current of latest developments

Topics

- Legal framework
- Search engine abuse
- Internet service spam
- Account hijacking
- Malware

Syllabus

1 Course Information

Web page: https://courses.engr.illinois.edu/ece498kl/fa2018
Piazza: https://piazza.com/illinois/fall2018/ece498kl
Term: **October 25, 2018** to **December 11, 2018**

Lectures: Tuesdays and Thursdays, 2:00 P.M. to 3:20 P.M. in ECEB 2015
Final exam: December 14, 8:00 A.M. in ECEB 2015

Instructor: Kirill Levchenko
Email: klevchen@illinois.edu
Office hours: Mondays at 2:00 P.M. in CSL 468

Teaching Assistant: Joshua Reynolds
Email: joshuar3@illinois.edu
Office hours: Thursdays at 1:00 P.M. in CSL 221

Prerequisites

- ECE 391 or CSE 241
- Networking (or learn quickly as you go)
- You will need to know some PHP, JavaScript and a language for network programming
  (Java, C/C++, Python, etc.)

Grading

- 10 quizzes — *one each lecture* (30% of grade)
- 7 programming assignments (40% of grade)
- Final exam (30% of grade)

Lectures

- Lecture slides will be available online
- Complete assigned readings *before* lecture
  - We will use lecture time to discuss the material
- Lectures are interactive — ask questions
  - Your questions (and feedback) will help improve the course!

Reading Questions

- Each reading will have set of Reading Questions
- Lecture will focus on these questions
  - Cover core ideas of the reading
- Guideposts to understanding material
- You should be able to answer these after reading

Quizzes

- 5-minute quiz at the beginning on every lecture
  - **No make-up quizzes:** *must be in class to take quiz*
- Quiz covers assigned reading
  - Expect to get 100% if you did the reading
- Lowest quiz grade dropped
- ***Note:*** reading questions ≠ quiz questions

Assignment Policy

- Assignments due on date and time indicated
  - Assignment 1 Part A due October 30 by 10 PM
- Must be submitted electronically
  - Details in assignment
- You have three 24-hour extensions
  - Debited in 24-hour increments when assignment is late
  - When you run out, late assignments *will not be accepted*
  - **No other extensions will be granted**

Academic Integrity

- Read and understand University of Illinois policy
  - `http://studentcode.illinois.edu/article1_part4_1-401.html`
- There will be zero tolerance for cheating
  - Computer security requires the utmost individual integrity
- Is it ok to post your solutions to an assignment?

single experiment for several more required analyses.
(2) Altering the answers given for an exam after the examination has been graded.
(3) Providing false or misleading information for the purpose of gaining an academic advantage.

(d) Facilitating Infractions of Academic Integrity. No student shall help or attempt to help another to commit an infraction of academic integrity, where one knows or should know that through one's acts or omissions such an infraction may be facilitated. A violation of this section includes but is not limited to:
(1) Allowing another to copy from one's work.
(2) Taking an exam by proxy for someone else. This is an infraction of academic integrity on the part of both the student enrolled in the course and the proxy or substitute.
(3) Removing an examination or quiz from a classroom, faculty office, or other facility without authorization.

Academic Integrity

- Read and understand University of Illinois policy
  - `http://studentcode.illinois.edu/article1_part4_1-401.html`
- There will be zero tolerance for cheating
  - Computer security requires the utmost individual integrity
- Is it ok to post your solutions to an assignment? **No.**
- Not sure? *Ask instructor or TA*

Assignment Set 1

- Deceptive Search Engine Optimization and Web attacks
- Run a Web site and collect data on visits (Parts A & B)
- Cloak your site from search engines (Part C)
  - Search engines see one version of site
  - Users see another version of site
  - Used to lure users into visiting cite
- **Part A due October 30** — *start now!*

Assignment 2

- Spam a Web site operated by Instructor and TA
- Must circumvent site anti-spam defenses
  - Becomes increasingly harder (Parts B & C)
- **Part A due November 15** (tentative)


ECE 498KL ECRIME AND INTERNET SERVICE ABUSE
MASS:WERK DATA CENTER <masswerk.at>
CDL 0815

Questions?

What is E-Crime?

Crime and Law

- **What is a crime?**
  Offenses prohibited by law prosecuted by the state
- **What is Law?**
  - **Statutes:** laws passed by legislative body (e.g. Congress)
  - **Common law:** Judicial precedent including elements inherited from English courts
  - **Regulations:** Rules made by executive agencies based on statutory authority

THE THREE BRANCHES OF GOVERNMENT

THE US CONSTITUTION

The framers of the Constitution wanted to be sure that no one person or group had too much power. They created a system of checks and balances. They separated the government into three branches. The three branches are separate but equal. Each branch can "check" the power of the other branches. The three branches work together to govern our nation.

LEGISLATIVE
makes laws

EXECUTIVE
carries out laws

JUDICIAL
evaluates laws

CONGRESS

Senate

100 SENATORS

- elected every 6 years
- must be at least 30 years old, must have been a US citizen for at least 9 years, and must live in the state they represent

House of Representatives

435 REPRESENTATIVES

- elected every 2 years
- must be at least 25 years old, must have been a US citizen for at least 7 years, and must live in the state they represent

PRESIDENT

- elected every 4 years
- must be at least 35 years old, a US citizen, and must have lived within the US for at least 14 years

Vice President

Cabinet

SUPREME COURT

9 Justices

- nominated by the president and confirmed by a majority Senate vote
- hold office as long as they choose to stay

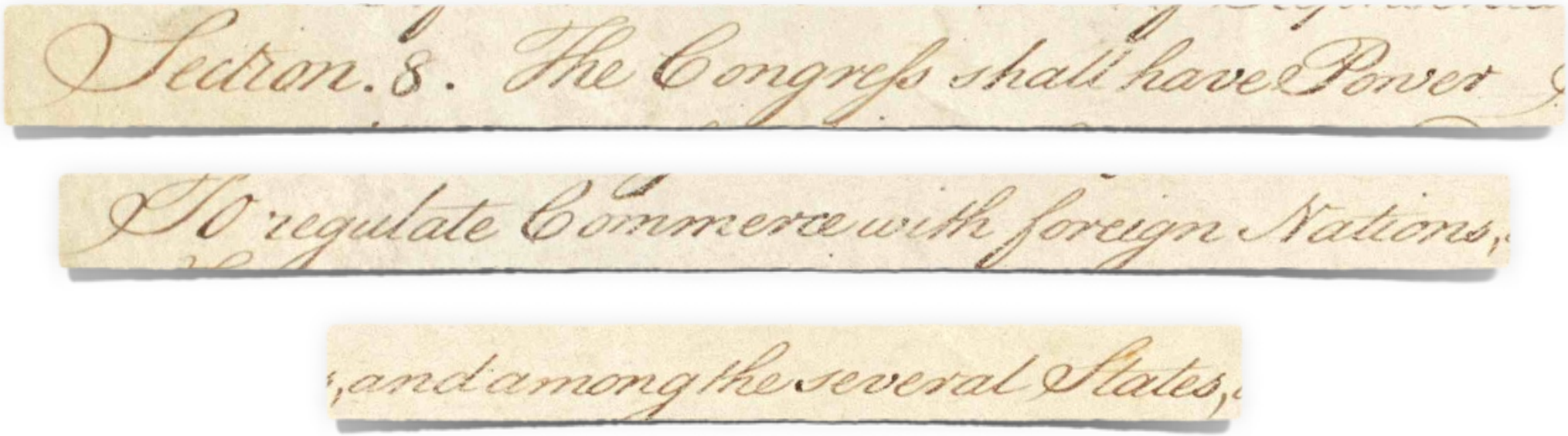
other Federal Courts

Statutes

- **Federal laws** enacted by U.S. Congress
  - **Illinois US Senators:** Tammy Duckworth (D) and **Dick Durbin** (D)
  - **Illinois 13th Congressional district Rep.:** Rodney Davis (R)
- **State laws** enacted by state legislatures
  - **Illinois Senate District 52 Senator:** Scott M. Bennett (D)
  - **Illinois House District 103 Rep.:** Carol Ammons (D)
- **Local:** usually city ordinances enacted by a city council

Federal vs State

- US Constitution leaves a lot up to the States
  - In principle Congress' authority is limited to Federal issues
- Commerce Clause of US Constitution gives Congress authority to *regulate interstate commerce*



The Congress shall have Power …
To regulate Commerce with foreign Nations,
and among the several States …

Federal vs State

- US Constitution leaves a lot up to the States
  - In principle Congress' authority is limited to Federal issues
- Commerce Clause of US Constitution gives Congress authority to *regulate interstate commerce*
- Today the Commerce Clause interpreted very broadly
  - In practice Congress enjoys vast authority …
    … including laws about to e-crime

US Code

- **US Code:** current body of laws enacted by US Congress
- Updated by acts of Congress (legislation)
  - **US Code** analogous to current version of software
  - **Acts of Congress** analogous to patches applied to codebase
- Acts of Congress often modify several parts of US Code

E-Crime

- Computer crimes covered by Federal and State laws
- Federal computer crime statutes
  - Computer Fraud and Abuse Act (CFAA) — Oct 30
  - Electronic Communications Privacy Act (ECPA) — Nov 1
  - Stored Communications Act (SCA) — Nov 1
  - Digital Millenium Copyright Act (DMCA)
- Illinois State computer crime statutes
  - Illinois Computer Crime Prevention Law (ICCPL)

Criminal Procedure

- *What happens when you break a law?*
- Arrested by agency responsible for enforcing the law
  - Federal e-crime laws usually enforced by FBI
- Charged with committing crime
- Trial to determine guilt or innocence

The Courts

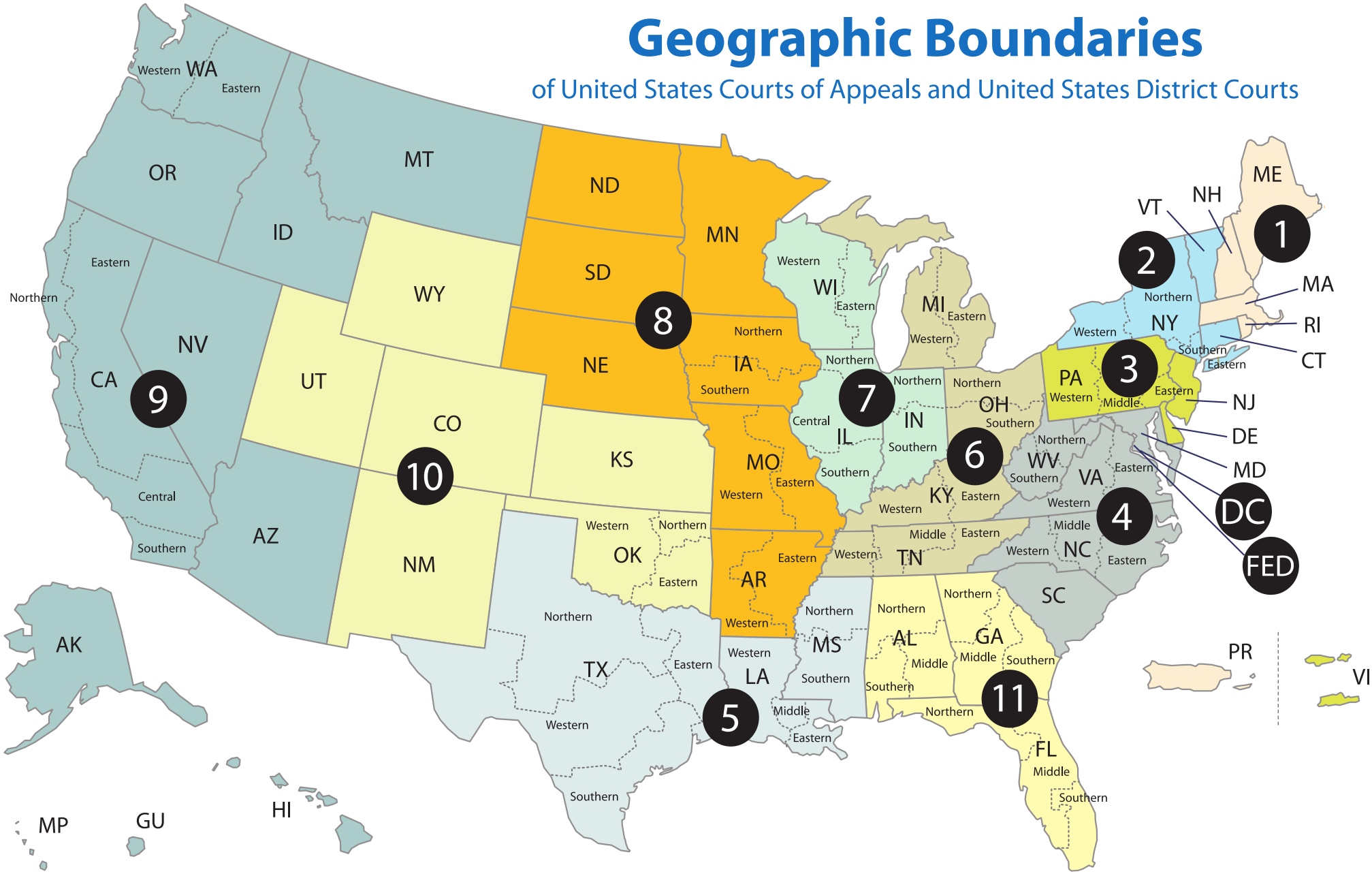
- Laws are interpreted by the Courts
  - **State Courts** (for state laws)
  - **Federal Courts** (for federal laws)
- Courts should interpret laws *consistently*
- **Precedent:** established interpretation of law
  - Lower courts *must* follow precedent set by higher courts
  - Court may overturn its own precedent (rare)

US Federal Courts

- Supreme Court of the United States
  - Nine Supreme Court justices
- 13 Courts of Appeal (Circuit Courts)
  - 12 regional and 1 Federal Circuit
  - May have conflicting interpretations of law
- 94 District Courts

Geographic Boundaries

of United States Courts of Appeals and United States District Courts



Civil vs Criminal

- Crimes are prosecuted by the state ("the people")
  - **Misdemeanor:** Punishable by up to one year in jail or prison
  - **Felony:** Punishable by more than a year in prison
- Civil lawsuits may be brought by individuals
  - Resolve contract disputes, recover loss, remedy harm
  - Individuals may seek to compel compliance with law
  - Some statutes allow individuals to seek damages

Reading Assignment

- **18 U.S. Code § 1030 —**
  Fraud and related activity in connection with computers
- Federal statute (passed by US Congress)
- Law that criminalizes “hacking”
- Authority stems from Commerce Clause
  - Note references to “interstate commerce” as you read

18 U.S. Code § 1030 - Fraud and related activity in connection with computers

(a) Whoever—

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n)

[1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

Amendments

2008—Subsec. (a)(2)(C). Pub. L. 110–326, § 203, struck out "if the conduct involved an interstate or foreign communication" after "computer".

Subsec. (a)(5). Pub. L. 110–326, § 204(a)(1), redesignated cls. (i) to (iii) of subpar. (A) as subpars. (A) to (C), respectively, substituted "damage and loss." for "damage; and" in subpar. (C), and struck out former subpar. (B) which read as follows:

"(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)—

"(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

"(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

"(iii) physical injury to any person;

"(iv) a threat to public health or safety; or

"(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;".

Subsec. (a)(7). Pub. L. 110–326, § 205, amended par. (7) generally. Prior to amendment, par. (7) read as follows: "with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;".

Subsec. (b). Pub. L. 110–326, § 206, inserted "conspires to commit or" after "Whoever".

Subsec. (c)(2)(A). Pub. L. 110–326, § 204(a)(2)(A), struck out "(a)(5)(A)(iii)," after "(a)(3),".

Subsec. (c)(3)(B). Pub. L. 110–326, § 204(a)(2)(B), struck out "(a)(5)(A)(iii)," after "(a)(4),".

Subsec. (c)(4). Pub. L. 110–326, § 204(a)(2)(C), amended par. (4) generally. Prior to amendment, par. (4) related to fines and imprisonment for intentionally or recklessly causing damage to a protected computer without authorization.

Subsec. (c)(5). Pub. L. 110–326, § 204(a)(2)(D), struck out par. (5) which related to fine or imprisonment for knowingly or recklessly causing or attempting to cause serious bodily injury or death from certain conduct damaging a protected