Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 3: The Ethical Hacker

1. The use of information technology to gain unauthorized access to computer systems or password protected sites is known as:
   a. Hacking
   b. Piracy
   c. Cybertrespass
   d. Computer fraud
2. The use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data is known as:
   a. Cybersabotage
   b. Cyber warfare
   c. Targeting critical infrastructure
   d. Cybervandalism
3. The use of deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data is known as:
   a. A data breach
   b. Computer fraud
   c. Cybertheft
   d. Unethical hacking
4. The execution of politically motivated hacking operations intended to cause grave harm that is, resulting in either loss of life or severe economic loss or both is known as:
   a. Phishing
   b. Bug bounty hunting
   c. Cyberterrorism
   d. Cyberwarfare
5. The __________________ notes that breaking into federal computers may fall under definitions of terrorism and cyberhackers can be prosecuted as terrorists.
   a. Wassenaar Agreement
   b. Tallinn Manual
   c. US Patriot Act
   d. Computer Fraud and Abuse Act (CFAA)
6. IN Great Britain, the _____________________ listed engaging in computer hacking or threatening to engage in computer hacking as a potential terrorist act.
   a. Terrorism Act of 2000
   b. Terrorism Act of 2005
   c. Cyberterrorism Act of 2003
   d. UK Patriot Act

7. In considering the ethics of password sharing for streaming services, a _______________ would argue that the most expeditious outcome is one where the maximum number of people allowed or permitted enjoy the programming.

   a. Utilitarian

   b. Deontologist

   c. Virtue Ethicist

   d. Pragmatist

8. In considering the ethics of password sharing for streaming services, a _________________ would consider how we might react if a similar action was taken against us.

   a. Utilitarian

   b. Deontologist

   c. Consequentialist

   d. Pragmatist

9. Using and sharing cheat codes on video games is referred to as ______________.

   a. Crime

   b. Easter egging

   c. Activism

   d. Nuisance Hacking

10. Attacks on Critical Infrastructure would be viewed as _____________.

    a. Acts of War

    b. Psychological warfare

    c. DDoS attacks

    d. SCADA attacks

11. True or False:

    The new hacker ethics includes the understanding that the physical world and the cyber world are separate. (FALSE)

12. True or False:

    A black-hat hacker works for or with a private corporation or government to test their systems' security. (FALSE)

13. Malware which can be surreptitiously loaded onto a computer with the ability to encrypt all of a user's files is known as:

    a. Botnets

    b. Ransomware

    c. A worm

    d. A virus

14. The 2016 US Department of Defense "Hack the Pentagon" initiative is an example of a:

    a. Bug bounty program

    b. Act of War

    c. Nuisance hacking competition

    d. White-hat hacker incentive program

Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 4: The Problem of Privacy

1. The right not to be observed or to be left alone is referred to as:
    a. Physical privacy
    b. Decision privacy
    c. Autonomy
    d. Sovereignty
2. The right to make decisions about your own life without interference by others is referred to as:
    a. Mental privacy
    b. Decision privacy
    c. Emancipation
    d. Sovereignty
3. The ability to have our own thoughts is known as:
    a. Academic freedom
    b. Freedom of speech
    c. Mental privacy
    d. Autonomy
4. The right to control what others known about you and what information is collected and shared about you is known as:
    a. Data privacy
    b. Data autonomy
    c. Information privacy
    d. Information sharing autonomy
5. The distinction between public and private information can be traced back to:
    a. Emmanuel Kant
    b. John Locke
    c. Jean-Jacques Rousseau
    d. Aristotle
6. Legislation enacted in France stating that employees cannot be required to respond to work e-mails during their leisure time rests on the principle of:
    a. Autonomy
    b. Surveillance
    c. Wage equality
    d. Worker Sovereignty
7. A US federal law which regulates the privacy of student educational records is referred to as:
    a. FERPA
    b. The Hippocratic oath
    c. HIPAA
    d. The information privacy act

8. The great ethical challenge today is in preserving ____________ while providing _________.
   - a. Privacy; security
   - b. Security; autonomy
   - c. Data; privacy
   - d. Sovereignty; transparency
9. The reliance on a group of characteristics (which are) believed to be associated with crime by law enforcement officers is referred to as:
   - a. Differential surveillance
   - b. Criminal surveillance
   - c. Criminal profiling
   - d. Data analytics
10. True or false: The Right to Be Forgotten is an established legal principle in the United States. (FALSE)
11. ____________ refers to a system in which some individuals are monitored or surveilled more closely than others.
    - a. Racism
    - b. Tiered privacy
    - c. Privacy calculus
    - d. Data profiling
12. The proactive integration of technical privacy principles in a system's design is referred to as:
    - a. Privacy by design
    - b. Security by design
    - c. Designer's intent
    - d. Social construction of technology
13. True or False: Some analysts argue that privacy is a social construct which varies widely across time and across cultures. (TRUE)
14. True or False: The field of encryption rests on the assumption that privacy is absolute and that we have an absolute right to keep secrets (FALSE)
15. The principle that just because one has the power to do something, one can still discipline oneself not to do it is known as:
    - a. Restraint
    - b. Submission
    - c. Surrender
    - d. Magnitude

Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 5: The Problem of Surveillance

1. The Dutch initiative to encourage citizens to photograph and record possible criminal acts is known as:
   a. Participatory surveillance
   b. Differential surveillance
   c. Ubiquitous surveillance
   d. The Internet of Things
2. The use of a scanner at the airport, along with the use of biometrics or access control cards is an example of:
   a. Workplace security
   b. Obtrusive detection
   c. Detection from a distance
   d. Information privacy regimes
3. The use of algorithms to monitor employee behavior within an organization is aimed at identifying:
   a. Insider threats
   b. Encryption violators
   c. White hat hackers
   d. Obtrusive detection
4. A situation where someone is legally accountable or liable for a criminal offense based upon the behavior of another is known as:
   a. Complicity
   b. Health surveillance
   c. Data interdependence
   d. Activity interdependence
5. Technologies which have both civilian commercial and military uses are known as:
   a. Dual-hatted technologies
   b. Dual use technologies
   c. Export regime technologies
   d. Emerging technologies
6. True or False:
   The United States has successfully extended the terms of the Wassenaar Arrangement to include cyberweapons among the items controlled by export regimes. (FALSE)
7. True or False: Jeremy Bentham was one of the first utilitarian philosophers (TRUE)
8. True or False: Mutual Legal Assistance Treaties require nations to assist one another in carrying out criminal prosecutions. (FALSE)
9. True or False: The Foreign Intelligence Surveillance Act of 1978 established the principle that in a free society, states cannot monitor the internal communications of their citizens. (FALSE)

10. __________________ involves acts intended to kill, injure, harass or cause substantial emotional distress to another, using any interactive computer.
    a. Cyberstalking
    b. Emotional blackmail
    c. Information warfare
    d. Cybercrime
11. _____________ refers to “repeated threatening or harassing e-mail messages, instant messages, blog entries or websites dedicated solely to tormenting an individual.”
    a. Cyberstalking
    b. Cyber harassment
    c. Perfidy
    d. Psychological warfare
12. True or False:
    The principle of transparency is a key element in making sure governments and corporations are accountable to people. (TRUE)
13. True or False: Bitcoin is not issued by a central bank. (TRUE)
14. True or False: Individuals who believe that they are the subjects of surveillance may begin to alter their own behavior and self-perception as a result. (TRUE)
15. True or False: At the moment, Europe has better and more thorough privacy laws than the United States. (True)

Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 6: The Problem of Piracy

1. An ___________ is the right to be financially compensated if someone else uses your intellectual property.
   a. Patent
   b. Statute
   c. Economic right
   d. Civil penalty
2. A ______________ is the right to be recognized as the creator of the idea or concept.
   a. Fair Use
   b. Moral right
   c. Patent
   d. Copyright
3. True or False: The notion of intellectual property is fairly recent, and can be dated back to the advent of the internet (FALSE)
4. The term ______________ refers to practices by which individuals upload or download, share, transmit or distribute audio or visual information files which are copyrighted.
   a. Cloning
   b. Information theft
   c. Piracy
   d. Patent
5. ___________ argues that you earn the right of ownership through taking an object (like farmland) and "mixing (your) labor with it."
   a. Jeremy Bentham
   b. John Locke
   c. Emmanuel Kant
   d. Michel Foucault
6. True-False: The principle of genetic exceptionalism establishes the principle that genetic material information is even more entitled to privacy protections than other forms of data (TRUE)
7. The notion that your actions and values should be consistent across environments is known as:
   a. Transparency
   b. ubiquity
   c. Data complicity
   d. Integrity
8. True/False: There are no legitimate, lawful reasons why an individual or state would ever utilize a bullet proof hosting service. (FALSE)
9. True/False: A citizen in a Western democracy would likely oppose the Asian mindset of shared assets in relation to intellectual property. (TRUE)

10. AN argument stating that any gains which an individual accrues through piracy are outweighed by the damage to the collective which ensues is most likely to be made by:
    a. A virtue ethicist
    b. A deontologist ethicist
    c. A moral absolutist
    d. A utilitarian
11. True or False: The 2003 United States Can-Spam Act has virtually eliminated the problem of spam e-mails in the US. (FALSE)
12. A unit of cultural material that spreads virally, passed from person to person via electronic means is known as:
    a. A meme
    b. A worm
    c. A trojan
    d. A snail
13. The term ______________ refers to non-copyrighted intellectual property that can be copied and freely distributed (but not sold) by anyone without payment or permission.
    a. Meme
    b. Open source
    c. Public domain
    d. Cloned material
14. True/False: Work produced under a Creative Commons license can be used by anyone without paying for it. (TRUE)
15. One group particularly likely to engage in piracy is:
    a. College students
    b. Older, less technologically savvy individuals
    c. Middle class individuals
    d. Engineers and technology personnel

Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 7: The Problem of Cyberwarfare

1. An extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare is known as:
   a. Information warfare
   b. Psychological operations
   c. Electronic warfare
   d. Disinformation
2. Warfare waged in space, including defending information and computer networks, deterring information attacks and denying an adversary's ability to do the same is known as:
   a. Cyberwarfare
   b. Mechanized warfare
   c. Space operations
   d. Electronic operations
3. True/False: The Tallinn Manual on the International Law Applicable to Cyber warfare was authored by the United States (False)
4. An action by one country against another with an intention to provoke a war or an action that occurs during a declared war or armed conflict between military forces of any origin is referred to as:
   a. An act of war
   b. A LOAC violation
   c. A just in bello violation
   d. Preemptive war
5. International Law has traditionally been based upon:
   a. The Geneva Convention
   b. The Law on Armed Conflict (LOAC)
   c. The Treaty of Versailles
   d. Both A and B
   e. Both A and C
   f. All of the above
6. _____________ is a set of understandings about what actions people can and cannot take during wars.
   a. Jus in bello
   b. Jus ad bellum
   c. Jus qua bellum
   d. Just war principles
7. _____________ describes the principles of what constitutes a Just War or one which is engaged in for the right reasons.
   a. Jus ad bellum
   b. Jus post bellum
   c. Law of Armed Conflict
   d. Jus in bello

8. The doctrines that states must use only enough force to accomplish their objective is known as:
   a. Proper Authority
   b. Proportionate Force
   c. Last Resort
   d. Just Cause
9. True or False: The Law of Armed Conflict places restrictions on the sites of attack, restricting armed forces from attacking civilian structures like hospitals and schools. (TRUE)
10. TRUE/FALSE: The Tallinn Manual states that a cyber attack can only be responded to with an in-kind attack. (FALSE)
11. True or False: One can make an ethical argument that cyberweapons are more ethical than conventional weapons since they are more precise in their aims. (TRUE)
12. The definition of a cyberweapon appears in:
   a. The Law of Armed Conflict (LOAC)
   b. The Tallinn Manual
   c. The USA Patriot Act
   d. NATO's founding documents
13. An attack carried out against critical national infrastructure is referred to as:
   a. An act of war
   b. A treaty violation
   c. A computer network attack
   d. Economic sabotage
14. The principle of _____________ refers to processes for identifying the perpetrator of an attack.
   a. Public-private cooperation
   b. Attribution
   c. Transparency
   d. Attack surveillance
15. True/False: Deception is legal under the Laws of Armed Conflict, which permits deceiving one's enemy through stratagems and ruses. (TRUE)

Review Questions for Mary Manjikian. Cybersecurity Ethics: An Introduction

Chapter 8: The Way Forward

1. True False: Engineers recommend that designers consider research problems from the viewpoint of the end user. (TRUE)
2. New technological developments which differ radically from those which preceded them are known as:
   a. Unique problems
   b. Novel Problems
   c. Unique technologies
   d. Emerging Technologies
3. The following activities represent a preemptive approach to considering information ethics:
   a. The European Commission Project of Ethical Issues of Emerging ICT Applications
   b. The NSF Future Internet Architecture Program
   c. The European Commission project on Future and Emerging Technologies
   d. All of the Above.

4. T/F The ACM Code of Ethics is based entirely on utilitarian principles. (FALSE)
5. The ethics for a research problem should be based on:
   a. The problem
   b. The engineer's own ethics
   c. The ethical issues which users may encounter
   d. All of the above
6. The US military views cyberspace as a _______________ of warfare.
   a. Arena
   b. Zone
   c. Domain
   d. Area
7. True/False: In the real world, a practitioner may find that he encounters multiple, conflicting sets of 'rules' for how to approach an ethical dilemma. (TRUE)
8. Engineering problems in the future are going to be increasingly:
   a. Interdisciplinary
   b. Regulated
   c. Preempted
   d. Straightforward
9. Three constraints which engineers may encounter in thinking about ethical issues in the future are:
   a. Organizational Culture, Legal Constraints and Time Constraints
   b. Salary requirements, organizational culture and legal constraints
   c. Legal constraints, staffing requirements and organizational culture
   d. Staffing requirements, salary requirements and organizational culture
10. True/False: One problem that developers face is a high level of technological literacy among consumers (FALSE)