Cyber Ethics

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Ethics vs Morals vs Law

Read: *Ethics vs Morals vs Law*, Dr. Arturo Perez

- https://www.linkedin.com/pulse/ethics-vs-morals-law-dr-arturo-perez
- You are responsible for knowing the concepts from the article

Definitions from the article:

- ***Ethics****: The moral principles that govern a person's behavior or the conducting of an activity.*
- ***Morals****: Concerned with the principles of right and wrong behavior and the goodness or badness of human character.*
- ***Law****: The system of rules that a particular country or community recognizes as regulating the actions of its members and may enforce by the imposition of penalties*

Also from the article:

- *Ethics and morals relate to "right" and "wrong" conduct. While they are sometimes used interchangeably, they are different: ethics refer to rules provided by an external source, e.g., codes of conduct in workplaces or principles in religions. Morals refer to an individual's own principles regarding right and wrong.*
- *Ethics comes from within a person's moral values. Laws are made with ethics as a guiding principle.*

Ethics vs Morals vs Law

As an example, one common question regarding time travel is:

- Would you go back in time and kill Adolph Hitler, before he rises to power?
- Murdering someone is illegal, but would it be ethical (or moral)?

What about tabloids?

- They might have photos or information about someone that they spin into a shocking (and potentially damaging) story to get clicks or sell magazines.
- Barring a few libel laws, this is probably legal. However, harming someone to make a profit is probably not ethical or moral.

What about social media that manipulate news feeds to change people's behavior to increase "user engagement"?

- If you haven't seen the documentary *The Social Dilemma*, it covers this topic quite well

Morality vs Ethics

Here is a slightly different view

Read: *What's the Difference Between Morality and Ethics?* By Cydney Grannan

- https://www.britannica.com/story/whats-the-difference-between-morality-and-ethics

Two quotes from the article:

- *Many people think of morality as something that's personal and normative, whereas ethics is the standards of "good and bad" distinguished by a certain community or social setting.*
- *Ultimately, the distinction between the two is as substantial as a line drawn in the sand.*

Basically, this area is hard for even professional ethicists and philosophers to navigate

- There are also complications due to ***situational ethics***:
  - This is where moral rules can change due to the circumstances
  - For example, a person might think stealing is wrong – but stealing is okay if they are stealing bread to feed their family
  - Or, murder is wrong – unless you are a time traveler stopping Adolph Hitler

What Is Ethics

Read: What is Ethics? By Velasquez, Andre, Shanks, and Meyer

- https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/what-is-ethics/

Key quotes from the article:

- *The meaning of "ethics" is hard to pin down, and the views many people have about ethics are shaky.*
- *But being ethical is clearly not a matter of following one's feelings. A person following his or her feelings may recoil from doing what is right. In fact, feelings frequently deviate from what is ethical.*
- *Nor should one identify ethics with religion.*
- *Being ethical is also not the same as following the law.*
- *What, then, is ethics? Ethics is two things. First, ethics refers to well-founded standards of right and wrong that prescribe what humans ought to do, usually in terms of rights, obligations, benefits to society, fairness, or specific virtues.*
- *Secondly, ethics refers to the study and development of one's ethical standards.*

Cyber Ethics

Read: Cyberethics, Wikipedia

- https://en.wikipedia.org/wiki/Cyberethics

Pay special attention to:

- The definition of Cyberethics
- The Code of Fair Information Practices
- Ten Commandments of Computer Ethics
- ***You should be able to recognize their principles if they were presented to you***

Cyber ethics covers a lot of different technical areas:

- Artificial intelligence
- Privacy
- Intellectual property
- Free speech
- Anonymity
- Environmentalism (Ex: Impact of cryptocurrencies on energy usage)

ACM Code of Ethics

Read: *ACM Code of Ethics and Professional Conduct*, Association for Computing Machinery

- https://www.acm.org/code-of-ethics
- You are responsible for being familiar with the main points in the Code of Ethics

One reason to have a code of ethics for “cyber professionals” is that they are given tremendous responsibility (and power) with their positions

- For example, a database administrator (DBA) for Best Buy could (in theory) pull deliver information for expensive audio-video equipment and sell that to organized crime
- The same DBA could manipulate invoices to make it look like all their friends purchased a protection plan when they didn’t
- A developer could copy all credit card information prior to being encrypted
- In a medical setting, someone could manipulate medical information to make sure someone is given the wrong medication – with potentially fatal consequences

As we saw in the last lesson:

- ***From Marvel’s Spider-man: “With great power must also come… great responsibility!”***

(ISC)^2 Code of Ethics

Read: *Code of Ethics*, (ISC)^2

- https://www.isc2.org/Ethics
- ***As with the ACM Code of Ethics, you are responsible for being familiar with the main points in the Code of Ethics***

Notice that the (ISC)^2 Code of Ethics is much shorter than the ACM Code of Ethics

However, also note that there are many similarities between the two:

- (ISC)^2 :
  - *Protect society, the common good, necessary public trust and confidence, and the infrastructure.*
  - *Provide diligent and competent service to principals.*
- ACM Code of Ethics:
  - *Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.*
  - *Strive to achieve high quality in both the processes and products of professional work.*

Computer Professionals for Social Responsibility

A historical group regarding ethical conduct was the Computer Professionals for Social Responsibility (CSPR)

This was, according to Wikipedia:

- *A global organization promoting the responsible use of computer technology. CPSR was incorporated in 1983 following discussions and organizing that began in 1981.*
- https://en.wikipedia.org/wiki/Computer_Professionals_for_Social_Responsibility

They were primarily concerned about the use of computers (and artificial intelligence) in warfare

- Specifically, the use of A.I. in military systems (the Strategic Computing Initiative)

They were disbanded in 2013

- Of course, the use of information technology in warfare has greatly increased since then

However, this organization does give us an interesting question:

- When is it ethical to use computers in warfare?

Ethics and Cyberwarfare

One question could be:

- When is it okay to use a zero-day (or any exploit) against the civil infrastructure of another country?

Should cyber weapons be considered just another weapon?

If an attack could take down the power grid for an entire country, should it be treated like a nuclear weapon?

- What is the threshold for being considered a weapon of mass destructions?
- Is a small power outage, for a short period of time different than taking down a grid (and medical facilities) for weeks?

Ethics and Cyberwarfare

This are is a large area of uncertainty, but here are a few principles from nuclear strategy:

Launch on Warning (LOW): This is where a counter-attack is a strategy of nuclear weapon retaliation that gained recognition during the Cold War between the United States and the Soviet Union

- With the invention of intercontinental ballistic missiles (ICBMs), launch on warning became an integral part of mutually assured destruction (MAD) theory
- Under the strategy, a retaliatory strike is launched upon warning of enemy nuclear attack while its missiles are still in the air and before detonation occurs
- Basically, don't launch your cyber weapons first – but be ready to in case the enemy does

There is limited guidance from international law:

- ***Self-Defense***: You're not supposed to indiscriminately engage in war with other nations, but you are allowed to defend yourself.
  - But what is self-defense in cyberwarfare?
- ***Proportionality***: The objective is to try and limit the scope of a conflict and not let it escalate.
  - How you respond should be equivalent to how you were attacked (in effect if not in the method).
- ***Limitations on Targets***: What are acceptable targets?
  - This is especially true in the cyber arena where so much of the cyber infrastructure is shared between military and civilian functions.

Black, Gray, and White Hats

One way that hackers are differentiated is by the color of their hats – like in old Western movies

- The good guy wears a white hat
- The bad guy wears a black hat
- However, since real life isn’t as clearly defined, we also have the gray hats

White hat hackers are also commonly referred to as “Ethical Hackers”

Black hat hackers are also referred to as “Cyber Criminals”

Gray hat hackers – are in-between the two

- In some ways they act like a white hat, but in others like a black hat

Black, Gray, and White Hats

Read: Black hat, White hat, and Gray hat hackers – Definition and Explanation, by Kaspersky

- https://www.kaspersky.com/resource-center/definitions/hacker-hat-types
- You are responsible for the definitions of the various hats, what they are, and how they work

Key point from the article regarding black vs. white hats:

- *The main difference between the two is motivation. Unlike black hat hackers, who access systems illegally, with malicious intent, and often for personal gain, white hat hackers work with companies to help identify weaknesses in their systems and make corresponding updates. They do this to ensure that black hat hackers cannot access the system's data illegally.*

One Final Note

Just remember that the ability to do something doesn’t mean that you have permission to do it

- For example, if a teenager has a 10:00 p.m. curfew, they have the ability to stay out later – but they definitely don’t have permission to do so

Like our earlier points on responsibility – just because you have access to files, databases, information, and resources, that doesn’t mean you have the permission to do anything you want with them

- For example, you may be capable of using your work systems to mine Bitcoin or other cryptocurrency – but your employer probably hasn’t given you permission to use their hardware, cooling infrastructure, and electricity for your own gain
- You could also use business information from an employer to create your own business and steal a lot of customers – but that would probably be unethical and illegal