Cyber Security Ethics

Ethics is defined as a set of moral principles that direct a person's behavior especially when they are conducting an activity. In John Locke's work, he wrote about how humans are influenced by their environment. Morality can come from a varying range of sources, and it's what truly makes humans unique from one another. In the current state of cybersecurity, there are differing views on this topic.

The Tallinn Manual was first posted in a series of responses to Russian cyberattacks on Estonia in 2008. The purpose of the manual was to create a basis for how nation-states would approach cyber operations both conducted and directed against states. The manual defines a threshold for a state to defend itself when cyber operations cause injury, death, and destruction. The state being targeted can take action in a proportionate response. It is also worth mentioning that the manual attempts to highlight the dangers of escalating cyber warfare.

This framework was adopted by many nations, however, opponents denounced the Tallinn manual for not being applicable. Since the manual is not legally binding, many criticize it for being a western academic exercise that isn't appropriate for the majority of nation-states. The manual does not address power dynamics meaning a cyber attack could have different proportionality impacts between nations. It is also worth mentioning that the manual does not acknowledge cultural differences between nations, which creates an echo chamber. The manual attempts to justify Jus ad Bellum, which means the conditions under which States may resort to war or the use of armed force in general. The problem is many cultures have different thresholds and priorities as to when it is appropriate to go to war. The lack of representation will stunt any further advancements to create an international standard that would appeal to all nations.

The concept of hacking back basically states that a party will retaliate with a cyberattack. This is a controversial ethical issue regarding cyber security, and the best action plan depends on the case. The first thing to mention about hacking back is the identity of the person or group that is going to operate. In the United States, if an individual or private organization is caught hacking back, this will most likely result in legal action. A nation-state on the other hand can perform cyber operations and may

have to worry about legal percussions from the international community depending on who the state is and what the kind of operation it is.

In the digital world, there are many cases where hacking back is necessary and could be considered self-defense. An example is looking at this issue from the perspective of a large company that has been attacked. Most companies will not be able to recover their lost assets, and in rare cases, hackers are caught and prosecuted. Law enforcement agencies have also been ineffective in both prosecuting and deterring cybercriminals. If a company can defend itself by hacking back, this can deter hackers from targeting the company.

There are also some major consequences to take into consideration if a party decides to hack back. First, it will set a precedent that hacking back will be tolerated, which can lead to endless cyber attacks. There are not many documents that standardize ethics. One of the problems with this topic is that there is a distinct view of ethics, meaning that many parties have different viewpoints. There is no clear definition of when it is justifiable to strike back, suggesting any argument could be used to give reasons to attack.

When conducting a cyberattack it is also worth mentioning who is affected by the attack. Every attack has consequences and it is worth taking into consideration who is affected. There are some cases where striking back may not be worth it due to the people it disproportionately affects.

In conclusion, there isn't a clearly defined code of ethics around cybersecurity when it comes to certain topics. Aristotle argued that humans gain everything they know through personal experiences from one’s environment. The world is a diverse place and It is in mankind's best interest to define a set of ethics around cyber operations or risk the dire consequence of endless cyberwarfare.

References:

Nature vs Nurture: http://experimental-origins.weebly.com/nature-vs-nurture.html

Hacking Back: http://solidsystemsllc.com/hack-back/

Tallinn Manual: https://www.youtube.com/watch?v=Xqjxy4Io2tY

Class Slides: https://classroom.google.com/u/1/w/NDUyMTMwODM3NTA5/tc/NDQ4MzUyODEyODM5

Tallinn Manual Explained: https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE