

Cyber Attacks and Retaliation

Amadeo Bellotti

Summary

- Cyber attacks at the Company as well as DoD level are more common than we think.
- A Committee met in June of last year and determined that not all attacks deserve retaliation
- New rules need to be put in place so that Countries have a treaty regarding cyberwarfare

Ethical Decision

- Identify ethical issue
 - a. Starting a war over cyber attacks
- Stakeholders
 - a. USA
 - b. Enemies of USA
 - c. Both want to gather Information without being caught
- Possible Solutions
 - a. Everyone has to give information to US
 - i. Pros: US knows about everyone
 - ii. Cons: US becomes hated

Ethical Decisions (cont.)

- Solutions (cont.)
 - a. No executes Cyber attacks
 - i. Pros: Nobody has US secrets
 - ii. Cons: We have no Secrets
 - b. We allow cyber attacks but you only retaliate for serious infractions
 - i. Pros: Information can be acquired
 - ii. Cons: Loss of information will occur
- Everyone will be permitted to use the last solution.
 - a. It treats people (countries) as ends

Ethical Decisions (cont.)

- The solution is in accord with nature
 - Not jumping straight into war is normal.
- The solution is a balanced approach because it doesn't make hypocrites out of one side.
- There would be a majority agreement because it allows some cyber attacks without war.
- I feel like this is the right solution
- Realism played the highest part in my solution because cyber attacks will always happen this way we can have a limit on it.

ACM Code

- Is actually against the idea of cyber attacks
 - 1.2: Avoid Harm to others
 - 1.7: Respect privacy of others
 - 2.5: Give analysis of possible risks
- If an agreement where in place...
 - 2.6 Honor contracts and agreements