Module 2 Journal Entry

Davis Plude
5/26/2025

The principles of science are important to how we investigate and understand the world around us and one of the key principles is **determinism**, which is the idea that things happen for specific reasons. In cybersecurity this means every break or failure has a cause like an out of date system or weak password. Another principle is **empiricism** which in cybersecurity terms means technicians rely on data to detect threats and confirm incidents. **Parsimony** calls for the simplest solution to be the best one. A cyber example is if a system is performing weird a simple misconfiguration is probably to blame before a cyber attack. **Objectivity** means setting aside personal bias, this is a crucial step in cybersecurity because thinking we are too obscure or small to be hacked can lead to bad practices that will get your systems compromised. **Ethical Neutrality** This principal says the idea of something doesn't judge right or wrong but studying it can help you understand. This is big in cybersecurity as researchers will study malware not to do harm but to understand how it moves, replicates, and infects. Lastly **relativism** means that scientific knowledge is ever changing and improving. This is important for cybersecurity professionals as new threats, exploits, and technologies are changing daily. This means ethical hackers and cybersecurity researchers have to keep up with the times and never stay stagnant in learning new technology. Together these scientific principals outline the cybersecurity method in how to defend and protect modern systems to the highest degree possible.

References

Umphlet, M. (2025). *CYSE201S Module 2* [Google Slides]. Canvas.