Module 2 Journal

Kayle Glaize
Jun 1 2026

Objectivity is basically the concept that science is a tool that is used to pursue and advance human knowledge and shouldn't be used to promote biases or personal interests (Reiss & Sprenger, 2020). An example of this in cybersecurity is when an analyst decides to review the evidence left behind after a major cyber-attack to find weakness in the system to later improve, instead of using the evidence to try to validate their own beliefs on the matter.

Parsimony is the principle of science that states that scientists should present their explanations as simply as possible. It's about avoiding any extra complexity that isn't absolutely required (Module 2 slides). An example of how this concept relates to cybersecurity is if a server goes down the explanation shouldn't imminently be that there must have been a catastrophic cyber-attack, instead the most simple and common causes should be checked first before jumping to conclusions.

The empiricism principle states that scientific knowledge can only come from evidence that we can observe with our senses through empirical research, and can't spawn from options, intuition, hunches, etc. (Module 2 Slides). An example of how this concept is used in cybersecurity is using system logs, user data, and other information/evidence to figure out the source cause of an incident.

The scientific principle of Ethical Neutrality is the principle in which investigation, research, analysis, testing, etc. must be done without the presence of bias. Basicity ensuring that a scientist's own personal beliefs don't interfere with them accurately conducting research (Module 2 Slides). An example of how this is used in cybersecurity could be a security analysis, despite having a good idea of who the culprit is, decided to conduct research on the source of a data breach instead of automatically making assumptions.

Determinism is the concept that everything is the direct result of previous events and actions. In other words, the reason you are who you are was directly determined and influenced by prior events, observations, and actions; that everything that has happened, happened as a direct result of something that has already happened (Britannica + Module 2 slides). An example of this concept in the world of cybersecurity is a hacker reverse engineering a system by studying how a computer responds to specific and predictable outcomes based on specific inputs.

Relativism is the idea that all things are related to one another and that everyone has a different perspective, and so every perspective and point of view should be treated as meaningful (Module 2 Slides) . A way this principle could be connected to cybersecurity is with the development of the internet and more advanced technology, new avenues for criminal activity online also opened. Because more crimes are being commented on digitally, computer-based security was invented.

References

Determinism | definition, philosophers, & facts | britannica. (n.d.). https://www.britannica.com/topic/determinism

Reiss, J., & Sprenger, J. (2020, October 30). *Scientific objectivity*. Stanford Encyclopedia of Philosophy. https://plato.stanford.edu/entries/scientific-objectivity/

Umphlet, Matthew (2026, June 1). *Principles of Social and Cybersecurity*. School of Cybersecurity, Old Dominion University. https://docs.google.com/presentation/d/1Jo7kMpaWztasW0enT8Nqlq6IIF-fo6ntzD7plF6Xvyg/edit?slide=id.p1#slide=id.p1