**Journal Entry 2**

Social sciences are just as scientific as natural sciences, so the scientific principles can be applied to cybersecurity through a framework of social science. The first principle, relativism, is about how things are related, meaning we must understand how different changes occur within one system and how it affects another. If we understand how these changes, or in this case technological changes, take place, we can understand behavioral dynamics, economic decisions, policy making, and social processes. The second principle, objectivity, is about how scientists study topics in a value-free manner. Our bias or opinions shouldn’t get in the way from asking questions related to cybersecurity and finding out what the facts are, since science is about advancing knowledge. Parsimony means scientists should keep their explanations simple. This is a lot harder to do in the social sciences because human behavior doesn’t always give us a definitive answer. Empiricism is about studying behavior that’s real to the senses, so relying on hunches or opinions may lead to erroneous conclusions about cybersecurity. Ethical neutrality is about ethical standards that scientists must follow to protect the rights of the people that are being studied. This can further our understanding of issues related to cybercrime and answer questions involving limited internet access to reduce cybercrime, police using digital technology to track human behavior, and many others. Determinism is about how behavior is caused, determined, or influenced by preceding events. Social scientists must ask questions related to why certain human behaviors related to cybercrime happen, and a middle ground between free will and determinism must be acknowledged.