So how do scientific principles of relativism, objectivity, parsimony, empiricism, ethical neutrality, and determination relate to cybersecurity? When considering relativism as it relates to cybersecurity it infers that all things are related and that changes made in one system can lead to changes in others. One example I like to use is in relation to the rise of digital extortion /ransomware-as-a-service model because of the development of global cyberspace and greater reliance on cloud-based network infrastructure. Or the refinement of laws, tools and techniques used by law enforcement to attribute and prosecute criminal organizations incentivized by the low-risk vs reward nature of digital extortion schemes. Objectivity plays an important role in the advancement of cybersecurity methods and technology. Driven by a need to advance knowledge rather than promote a particular opinion or point of view that can derail significant advancement in a particular field. It also hampers the ability to consider important implications of advancement in cybersecurity or related field like AI or data analytics and privacy. Parsimony is of course analogous to ensuring that the level of explanation is as simple as possible. An example of this would be the basic premise of cognitive fatigue as it relates to cybersecurity. That cyber fatigue is a weariness, or aversion to good cybersecurity behaviors or advice because of overexposure to complex cyber-related work demands or training. Easily digested and able to be related to others outside the fields of neuroscience and cybersecurity.

Empiricism plays a critical role in the advancement of the field of cybersecurity. Advances in cybersecurity strategies, tools and technology are driven by data collected through empirical research. Hunches and half formed opinions cannot capture the data required to test hypotheses, identify poor system design and vulnerabilities, or identify trends that drive investment in training and technology to maintain relevance in the industry. This goes hand in hand with ethical neutrality that I believe is crucial in the research, creation, and advancement of

future technology in the field of cybersecurity. Technologies like AI and data analytics pose significant threats to individual freedom and privacy if ethical standards aren't applied during research and development. Oversight and transparency after deployment is also a vital part of the ethical continuum that cannot be ignored. Finally, the principle of determinism provides a lens with which to understand current behaviors determined or influence by previous trends or events. An example related to cybersecurity could be the transition from physical to digital currencies used by criminal organizations today. Driven by lack of regulation and the ease with which they obfuscate the movement of large amounts of cryptocurrency without the level of scrutiny applied to global banking.