The principles of science including objectivity, parsimony, empiricism, ethical neutrality, and determinism are critical to addressing and understanding challenges in cybersecurity. Objectivity guarantees that cybersecurity professionals approach problems like network vulnerabilities or cyberattacks without bias, relying on factual evidence rather than opinions that could be subjective. Parsimony focuses on straightforward solutions to prevent intricate threats. Empiricism is evidence-based investigation where professionals rely on data and observation to identify, analyze, and mitigate threats successfully.

Robert Bierstedt (1970) argued that the social sciences adhere to the same principles as the natural sciences, making them equally scientific. This perspective is vital in cybersecurity, where human behavior and social patterns play major roles in developing online threats. Ethical neutrality and determinism are necessary for cybersecurity practices as well. Ethical neutrality allows professionals to examine cyberattacks or behaviors objectively, without moral judgement, to understand the root causes and implications. Determinism emphasizes that cyberattacks typically follow foreseeable patterns based on prior causes like system weaknesses or habits of the user, allowing professionals to create preemptive security measures. All of these scientific principles lay out a foundation for progressing cybersecurity strategies, guaranteeing they are effective, evidence-based, and adaptive to evolving threats.