

Principles of Science and How they relate to Cybersecurity.

Abdias Noel

June 1, 2026

The principles of science are foundational ideas that guide how scientific knowledge is developed, tested, and refined.

Relativism accepts that some truths, values, and knowledge can depend on cultural and social contexts. In cybersecurity, technical facts remain objective, but decisions about privacy, risk, and security priorities vary between organizations and countries.

Objectivism is the idea that facts exist independently of personal beliefs. For example, a sufficiently powerful brute-force attack can theoretically crack a password regardless of what people believe, even if doing so may be impractical.

Parsimony favors the simplest explanation that fits the evidence. In cybersecurity and digital forensics, investigators often begin with the most obvious explanation before considering more complex possibilities.

Empiricism states that knowledge should be based on observation, testing, and evidence rather than assumptions. Cybersecurity professionals apply empiricism through penetration testing, log analysis, packet captures, and incident investigations.

Ethical Neutrality holds that technology itself is neither good nor bad and that its ethical value depends on how it is used. For example, network scanners such as Nmap can be used by security professionals to identify vulnerabilities or by attackers to find targets.

Determinism states that events have causes and that the same causes under the same conditions should produce the same outcomes. In cybersecurity, troubleshooting relies on this principle, such as identifying a blocked Telnet connection as the result of a firewall rule or closed port.

Skepticism is the practice of questioning claims and requiring evidence before accepting them. In cybersecurity, skepticism is essential when investigating incidents, evaluating vendors, and diagnosing network problems.