

Sean Shreve

18APR2026

CYSE 200T

Professor Duvall

Discussion Board: The “Short Arm” of Predictive Knowledge

From this week's Jonas Reading: How should we approach the development of cyber-policy and infrastructure, given the “short arm” of predictive knowledge?

In earlier times, ethical frameworks had local, short term actions which primarily affected other individuals within small timeframe. When this standard was in place, moral responsibility only required limited foresight (Jonas 1973, p. 37). In other words, you only needed to care about the short term consequences of actions, because in reality at that time, that was truly the only aspects of life that were affected. This is what Hans Jonas called the "Short Arm" of predictive knowledge. However, as technology has developed to our now modern level, the nature of human action has fundamentally changed. Actions can now create consequences that extend far beyond the immediate present.

In regard to cyber policy and infrastructure operation in this modern era, actions can scale to much higher level and persist for long periods of time or indefinitely. Jonas details that our technical power now exceeds our ability to predict outcomes (Jonas 1973, p.39). We very well may not know what the true consequences of our genius will create, and ignorance can no longer serve as an ethical excuse. A few examples of these technical showcases of power are artificial intelligence, cloud ecosystems and critical infrastructure systems. These are truly a marvel of

emerging technological genius, but in cybersecurity these also create unpredictable second and third order effects.

Jonas describes a concept of ethical responsibility and foresight, which means prioritizing long term risk mitigation over short term efficiency or profit (Jonas 1973, pp. 40-43). Cyber-policy must adopt this concept and should incorporate cautionary principles, assume knowledge is incomplete, and anticipate unforeseen consequences. The early signs of Zero Trust adoption in organizations is an example, along with continuous monitoring and redundancy planning. In essence, developing cyber-policies and infrastructure that preserve stability, trust and security over time will stand on the highest ground in ethical responsibility.

References

Jonas, H. (1973). *Technology and responsibility: Reflections on the new tasks of ethics*. *Social Research*, 40(1), 31–54.