Chapter 3
The Crisis of Epistemic Regimes of Security: Intelligence, Techno-Populism, and Public Order

Alp Cenk Arslan
http://orcid.org/0000-0002-5526-2089
Turkish National Police Academy, Turkey

ABSTRACT

This chapter analyzes the structural crisis of public order in the Post-Truth Era, defined by the collapse of the state's monopoly on truth. It argues that the traditional epistemology of intelligence, rooted in verification, is being dismantled by the "affective epistemology" of techno-populism. Leveraging algorithmic governance and surveillance capitalism, these regimes replace verified expertise with data-driven emotion, fundamentally inverting the intelligence cycle. This epistemic rupture fabricates threats based on viral engagement rather than empirical reality, resulting in the securitization of identity politics while dangerously de-securitizing complex existential risks. Consequently, the state faces institutional paralysis, eroding trust, and rising vigilante security. The study posits that modern state survival depends on establishing "epistemic security", protecting the knowledge systems essential for rational governance against digital disinformation.

INTRODUCTION

The trajectory of modern statecraft has long been predicated on a singular, optimistic assumption, that the accumulation of information equates to the accumulation of security. For the better part of the late twentieth century, an era retrospectively

DOI: 10.4018/979-8-3373-6786-6.ch003

termed the Information Age, the governance of public order was anchored in the belief that uncertainty could be tamed through the rigorous collection, processing, and analysis of data. In this paradigm, the state acted as the ultimate arbiter of reality, utilizing its vast bureaucratic apparatus to distinguish signal from noise, fact from fiction, and genuine threat from mere rumor. Security was, in essence, a kinetic concept, defined by the physical protection of borders, critical infrastructure, and the citizenry from tangible harms.

However, as we advance deeper into the twenty-first century, this foundational stability has fractured. We have transitioned from an era defined by information scarcity and hierarchical control to a Post-Truth Era defined by information ubiquity, algorithmic volatility, and the erosion of shared objective reality. In this new chaotic landscape, the most profound threats to the state are no longer purely kinetic but are increasingly cognitive and ontological. Consequently, the mandate of public security has fundamentally expanded. It is no longer sufficient to merely ensure physical safety; the modern state must now grapple with the imperative of epistemic security, the security of the knowledge systems, verification mechanisms, and trust architectures upon which public order relies.

Epistemic security refers to the capacity of a political community to reliably identify threats, verify truth claims, and maintain a consensus on the nature of reality. Without this epistemic baseline, the operational mechanisms of the state, from law enforcement to emergency management, become paralyzed. If a society cannot agree on the existence of a pathogen, the validity of an election, or the source of a cyberattack, the very concept of public order disintegrates. The transition to the post-truth condition, therefore, represents a structural crisis of the security architecture itself. The map of the security environment, once drawn by professional analysts and updated through verified intelligence, is now being redrawn in real-time by algorithms that privilege outrage over accuracy.

Historically, the identification and verification of security threats were the exclusive preserve of established institutions. Following the Weberian tradition of the state's monopoly on the legitimate use of force, there existed a parallel monopoly on the legitimate definition of truth. Intelligence agencies, law enforcement bodies, and national security councils functioned as the gatekeepers of this truth. Operating within a closed-loop system, these institutions utilized verified data and established tradecraft to construct the threat landscape (Agırdil, 2025a; Agırdil, 2025b). Whether monitoring Cold War adversaries or tracking non-state terror actors, the process was linear and institutional: raw data was harvested, subjected to analytical rigor, and reproduced into actionable intelligence for policymakers (Acar, 2024).

Today, however, this institutional authority is facing an unprecedented challenge. The state's monopoly on defining security reality has been shattered by the democratization of information and the rise of digital platforms. We are witness-