Chapter 2
Structural Analysis of Cognitive Domains in Public Security Through a Voronoi Diagram and Eigenvector Centrality-Based Model

Onur Ağırdil
http://orcid.org/0000-0002-3544-2306
Turkish National Police Academy, Turkey

ABSTRACT

This study argues that public security today is shaped not only by physical threats but also by perception, trust, and sense-making processes that emerge within cognitive domains. With the rise of digitalization and the network society, information ecosystems have become fragmented, the ground of shared reality has weakened, and this has intensified risks such as social polarization, institutional distrust, radicalization, and societal violence. To analyze cognitive security risks, the study proposes an original model that combines the proximity-based spatial logic of Voronoi diagrams with the relational power analysis of eigenvector centrality. The model shows that small but structurally central actors can generate disproportionate influence, and that security risks should be assessed through structural centrality rather than visibility. Ultimately, the study recommends a public security approach that strengthens cognitive domain resilience and is grounded in legitimacy, transparency, and social trust, instead of intervention-centered policies.

DOI: 10.4018/979-8-3373-6786-6.ch002

INTRODUCTION

Public security has long been addressed as one of the most fundamental functions of the modern state within the framework of preventing physical threats and ensuring public order. Concrete risks such as crime, violence, terrorism, and public disorder have constituted the main reference points of security policies (Arslan, 2026). However, with digitalization, the rise of the network society, and the transformation of information ecosystems, this narrow framework of security has increasingly become insufficient. Today, processes that threaten public order often take shape in cognitive domains before becoming visible in the physical realm. This situation demonstrates that public security is not only an area that must be defended against material threats, but also against processes related to how reality is perceived and shared (Arslan 2025).

In recent years, the direct association of phenomena such as disinformation, social polarization, institutional distrust, and radicalization with public security indicates a significant shift in security studies. The increase in access to information can paradoxically fragment the ground of shared reality rather than strengthen it. The accelerated circulation of information through digital platforms leads individuals to attribute entirely different meanings to the same phenomena. In this context, public security now faces not only threats whose nature is known, but also phenomena whose meaning—what they are believed to be—has become uncertain. The weakening of the epistemic foundations of security directly affects the sustainability of public order (Arslan, 2021).

In the security literature, this transformation is explained through the sectoral and conceptual expansion of security. Moving beyond military- and law-enforcement-centered approaches, security has evolved to encompass social, political, economic, and ultimately cognitive dimensions. Cognitive domains have become the fundamental grounds where individuals' ways of making sense of the world are shaped, trust is produced, and legitimacy is constructed. Distortions occurring within these domains generate structural risks that cannot be compensated for by physical security measures alone. Consequently, public security has become not merely a matter of enforcing rules, but a matter of those rules being cognitively accepted.

The starting point of this study is the assumption that a significant portion of contemporary risks threatening public security are produced within cognitive domains. The impact of disinformation, perception operations, and alternative reality regimes is closely related not only to the existence of false information, but also to the network structures within which this information circulates, the actors through whom it spreads, and the trust relations it relies upon. For this reason, cognitive security requires a structural and relational perspective that goes beyond content analysis. In the existing literature, cognitive threats are often addressed at a norma-