

## Abstract

In an era marked by digital interconnection, the phenomenon of disinformation has evolved into a critical challenge to both individual and collective cognitive security. This thesis identifies disinformation as not merely a byproduct of the information age but as a tactical weapon, wielded by various state and non-state actors to influence, distort, and destabilize, with the potential to sway democratic processes. The current global landscape, characterized by polarization and hybrid warfare, has elevated the role of disinformation in exploiting vulnerabilities to erode societal trust and credibility. The thesis acknowledges the limitations of conventional security measures in countering disinformation, and instead advocates for translating proactive strategies from cybersecurity such as encryption, threat modelling, and constant monitoring into the cognitive security domain. A comprehensive, pioneering framework is proposed that integrates artificial intelligence, machine learning, cognitive psychology, and other disciplines, aiming to provide robust protection against disinformation's insidious effects. The proposed framework emphasizes privacy by design and insists on a strict data trail to mitigate abuse. Potential constraints, such as practical implementation hurdles, consent overhaul, resource allocation, and bias in data collection, are critically examined. Recommendations are outlined for continuous refinement, focusing on streamlined structures, proactive data collection approaches, explainable AI applications, and real-world testing. The thesis ultimately serves as a foundation for an ethically informed, proactive approach to safeguarding cognitive security in our interconnected world, recognizing the need for ongoing adaptability and refinement in the face of technological advancement and evolving disinformation tactics.