# ABSTRACT

Cybersecurity threats have evolved into complex and pervasive challenges, with state-sponsored cyberattacks posing significant risks to national security. This thesis examines the United States Department of Defense's (DOD) cyber strategy under the Biden administration in 2023, with a specific focus on addressing Russian cyber threats. This study employs the SolarWinds 2020 attack as a case study to analyze the strategic responses of the US DOD. The SolarWinds 2020 cyberattack, attributed to Russian actors, was a watershed moment in the realm of cyber threats. Its impact on numerous US government agencies and private organizations highlighted the urgency of an effective response. Through an in-depth examination of this case, this thesis seeks to understand the DOD's evolving approach to mitigating and countering such threats. The research employs a multidisciplinary approach, drawing on cyber policy analysis, national security studies, and case study methodology. It also incorporates an assessment of relevant policy documents, official statements, and actions undertaken by the Biden administration to shape the DOD's cyber strategy. This research provides a comprehensive overview of the evolving landscape of cyber threats and the measures taken by the US DOD to safeguard national security interests.

Keywords: Cyberstrategy, National Security, US Department of Defense (DOD), Biden Administration, Cyberattack