

## ABSTRAK

*Cyberwarfare*, sebagai bagian dari konflik siber modern dalam kajian keamanan non-tradisional, melibatkan penggunaan teknologi informasi dan komunikasi untuk mengganggu, merusak, atau menghancurkan infrastruktur dan sistem yang penting bagi negara target. Teori neorealisme, yang menekankan pentingnya kekuatan negara dan struktur sistem internasional dalam menentukan perilaku negara, menjadi kerangka teoritis utama untuk memahami dinamika kekuatan dan konflik di ruang siber antara China, Taiwan, dan Amerika Serikat. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus untuk mengeksplorasi berbagai insiden serangan siber, strategi, kebijakan, dan langkah-langkah pertahanan yang diambil oleh China, Taiwan, dan Amerika Serikat.

Hasil penelitian menunjukkan bahwa strategi *cyberwarfare* China terhadap Taiwan bertujuan untuk mempertahankan dan meningkatkan posisi hegemoniknya di kawasan Asia-Pasifik serta menantang dominasi Amerika Serikat dalam struktur internasional. Tindakan China meliputi serangan siber, infiltrasi sistem jaringan kritis, dan spionase yang bertujuan mengganggu stabilitas politik dan keamanan negara target terjadi setelah adanya aktifitas kerja sama siber Taiwan dan Amerika dalam rentang 2019 sampai 2020. Analisis dengan menggunakan teori neorealisme menunjukkan bahwa tindakan ini merupakan bagian dari strategi ofensif yang lebih luas untuk memperkuat posisi negosiasi China di sistem internasional dan melindungi kepentingan nasionalnya. Penelitian ini juga menggarisbawahi pentingnya memahami konteks struktural internasional dan kepentingan nasional dalam menganalisis konflik siber antarnegara melalui realisme struktural ofensif. Rekomendasi dari penelitian ini termasuk perlunya peningkatan kerja sama internasional dalam bidang keamanan siber dan pengembangan kebijakan yang responsif terhadap dinamika yang terus berkembang di ruang siber.

**Kata Kunci:** *cyberwarfare*, neorealisme, realisme struktural ofensif, keamanan siber

## **ABSTRACT**

*Cyberwarfare, as part of modern cyber conflict in non-traditional security studies, involves the use of information and communication technologies to disrupt, damage, or destroy infrastructure and systems critical to a target state. Neorealist theory, which emphasizes the importance of state power and the structure of the international system in determining state behavior, is the main theoretical framework for understanding the power dynamics and conflict in cyberspace between China, Taiwan, and the United States. This study uses a qualitative method with a case study approach to explore various cyber attack incidents, strategies, policies, and defense measures taken by China, Taiwan, and the United States.*

*The results show that China's cyberwarfare strategy against Taiwan aims to maintain and enhance its hegemonic position in the Asia-Pacific region and challenge the dominance of the United States in the international structure. China's actions include cyber attacks, infiltration of critical network systems, and espionage aimed at disrupting the political stability and security of the target country after Taiwan and the United States' cyber cooperation activities in the period 2019 to 2020. Analysis using neorealism theory shows that these actions are part of a broader offensive strategy to strengthen China's negotiating position in the international system and protect its national interests. This study also underlines the importance of understanding the international structural context and national interests in analyzing interstate cyber conflict through offensive structural realism. Recommendations from this study include the need to increase international cooperation in the field of cybersecurity and develop policies that are responsive to the ever-evolving dynamics in cyberspace.*

**Keywords:** *cyberwarfare, neorealism, offensive structural realism, cybersecurity*