IMPLEMENTASI *NATIONAL CYBER SECURITY PROGRAM* (NCSP) TAIWAN DALAM MERESPONS ANCAMAN SIBER TIONGKOK UNTUK MEMBANGUN STABILITAS EKONOMI DIGITAL (2019-2023)

ABSTRAK

Pesatnya transformasi digital di Taiwan menjadikannya salah satu pemain utama dalam ekonomi digital global sekaligus target ancaman siber yang semakin rumit, khususnya dari Tiongkok. Selama periode 2019-2023, intensitas serangan meningkat, berbarengan dengan pandemi COVID-19 dan ketegangan geopolitik, yang menimbulkan tekanan besar terhadap infrastruktur kritis, sektor semikonduktor, dan sistem informasi publik. Untuk merespons situasi tersebut, Taiwan mengimplementasikan *National Cyber Security Program* (NCSP) sebagai strategi utama dalam memperkuat pertahanan siber nasional dan menjaga keberlanjutan ekonomi digitalnya. Penelitian ini menganalisis bagaimana NCSP dijalankan sebagai respons strategis terhadap ancaman siber yang bersifat sistematis, mulai dari spionase hingga kampanye disinformasi. Dengan pendekatan kualitatif deskriptif dan studi literatur, serta kerangka teori keamanan non-tradisional, keamanan siber, kebijakan siber, dan ekonomi digital, penelitian ini menemukan bahwa NCSP fokus pada penguatan perlindungan infrastruktur informasi kritis, pengembangan industri keamanan siber dalam negeri, peningkatan kapasitas SDM, dan perluasan kerja sama internasional. Meski menunjukkan kemajuan kelembagaan dan respons yang adaptif, program ini masih menghadapi tantangan krusial seperti kekurangan talenta siber dan kesiapan menghadapi ancaman berbasis AI. Temuan ini memperlihatkan pentingnya integrasi antara keamanan dan pembangunan digital dalam merespons dinamika ancaman era digital, serta memberikan kontribusi bagi pengembangan studi dan kebijakan keamanan digital di tingkat nasional dan global.

Kata Kunci: Keamanan Siber, *National Cyber Security Program* (NCSP), Ekonomi Digital, Taiwan, Ancaman Siber Tiongkok

THE IMPLEMENTATION OF TAIWAN'S NATIONAL CYBER SECURITY PROGRAM (NCSP) IN RESPONDING TO CHINA'S CYBER THREATS TO BUILD DIGITAL ECONOMIC STABILITY (2019-2023)

ABSTRACT

Taiwan's rapid digital transformation has positioned it as a key player in the global digital economy, while also making it a prime target of increasingly complex cyber threats, particularly from China. Between 2019 and 2023, the intensity of these threats grew, coinciding with the COVID-19 pandemic and rising geopolitical tensions. These challenges placed significant pressure on Taiwan's critical infrastructure, semiconductor industry, and public information systems. In response, the Taiwanese government implemented the National Cyber Security Program (NCSP) as a central strategy to strengthen its national cyber defense and maintain the sustainability of its digital economy. This study examines how the NCSP was implemented as a strategic response to systematic cyber threats, ranging from espionage to large-scale disinformation campaigns. Using a qualitative descriptive approach and literature study, and grounded in the frameworks of non-traditional security, cybersecurity, cyber policy, and digital economy, the research finds that the NCSP focuses on strengthening the protection of critical information infrastructure, developing the domestic cybersecurity industry, improving human resource capacity, and expanding international cooperation. While the program has made institutional progress and shown adaptive responses, it still faces key challenges, particularly the cyber talent gap and preparedness for AI-based threats. These findings highlight the importance of integrating security and digital development to effectively address evolving threats in the digital era, and contribute to the broader discourse on cybersecurity policy and digital economy strategies at both national and global levels.

Keywords: Cybersecurity, National Cyber Security Program (NCSP), Digital Economy, Taiwan, Chinese Cyber Threats