Abstrak

Power dalam hubungan internasional telah begeser dari *physical domain* menuju *digital domain* melalui konsep *cyber power*, di mana kapasitas negara ditentukan oleh *network*, *software*, serta *human skill*. Mengacu pada kerangka multidimensional Joseph Nye Jr. dan pemikiran-pemikiran realisme, penelitian ini melihat bahwa kekuatan siber bukan hanya tentang penggunaan teknologi, tetapi akumulasi kebijakan-kebijakan yang terjalin pada tingkat individu hingga negara. Studi ini menggunakan metode kuantitatif untuk meninjau ketimpangan kekuatan siber antara Indonesia dan India, serta menelaah kebijakan yang berfokus pada pembentukan dan pengelolaan talenta keamanan siber sebagai elemen utama kekuatan nasional. Indonesia yang saat ini dipandang kurang optimal dalam melakukan pengembangan internal di sektor siber, dan India yang menunjukkan konsistensi dalam pembangunan talenta digital dan keamanan siber secara *massive* dan *multidimensional*, ditinjau melalui fenomena *digital literacy gap* sebagai ancaman terhadap *national security*, dengan asumsi bahwa individu dan masyarakat yang tidak memiliki literasi dan skill perlindungan diri dalam *cyberspace* akan melemahkan sistem pertahanan siber secara kolektif, yang pada akhirnya menghambat negara dalam mengakumulasi kekuatan sibernya untuk *exercising power* pada panggung hubungan internasional. Tesis ini menegaskan bahwa kekuatan siber Indonesia dapat diperbaiki melalui strategi asimetris berbasis pemanfaatan populasi dan pelatihan talenta siber secara masif secara *grass root*. Dengan memperkuat *human skills* melalui literasi digital, jalur vokasi, dan pelatihan intensif, Indonesia berpotensi membangun *reservoir* kapasitas manusia yang dapat menjadi fondasi *cyber power* yang lebih mandiri, kompetitif, dan berpengaruh. Penelitian ini berkontribusi pada kajian keamanan siber dalam disiplin hubungan internasional dengan menempatkan manusia sebagai inti dari pembentukan kekuatan siber sebuah negara.

Kata Kunci: Kekuatan Siber, Talenta Siber, *Human-Centric*

Abstract

Power in international relations has shifted from the physical domain to the digital domain through the concept of cyber power, where state capacity is determined by networks, software, and human skills. Drawing on the multidimensional framework of Joseph Nye Jr. and strands of realist thought, this research argues that cyber strength is not merely the use of technology, but the accumulation of interconnected policies spanning from the individual level to the state level. This study applies a quantitative approach to examine the disparity of cyber power between Indonesia and India, while analysing policies focused on the development and management of cybersecurity talent as a central element of national power. Indonesia which currently viewed as suboptimal in intensifying its internal cyber capacity, and India which demonstrates consistency in developing digital and cybersecurity talent in a systematic and multidimensional manner are evaluated through the lens of the digital literacy gap as a threat to national security, based on the assumption that individuals and societies lacking digital literacy and self-protection skills in cyberspace will collectively weaken cyber defence systems, ultimately preventing states from accumulating cyber power to exercise influence in the international arena. This thesis emphasizes that Indonesia's cyber power can be improved through asymmetric strategies based on population-driven and grassroots cyber talent development at scale. By strengthening human skills through digital literacy, vocational pathways, and intensive training, Indonesia has the potential to build a reservoir of human capacity that can serve as a more independent, competitive, and influential foundation for national cyber power. This research contributes to cyber security studies within the discipline of international relations by positioning humans as the central hub of a state's cyber power formation.

Keywords: Cyber Power, Cyber Talent, *Human-Centric*