Cyberterrorism dan Analisis Ancaman Keamanan Nasional = Cyberterrorism and the Analysis of National Security Threats

Barus, Faby Izaura Yulvahera, author

Abstrak

Tulisan ini mengkaji konsep cyberterrorism dalam konteks Indonesia, menggunakan pendekatan teoritis yang dikembangkan oleh Correia (2022) dan Prof. Golose (2015), serta berdasarkan kasus-kasus serangan siber aktual di negara tersebut. Studi ini memberi fokus pada karakteristik unik cyberterrorism yang mencakup aspek kognitif, di mana kerusakan di wilayah siber, korban, dan ancaman yang ditimbulkan menjadi kriteria penting dalam mengklasifikasikan jenis serangan. Correia mengidentifikasi bahwa cyberterrorism mencakup aktivitas siber yang mengajukan ideologi tertentu dan mengancam publik serta properti. Analisis kasus Bjorka, Polrileak, dan kebocoran data Bank Syariah Indonesia (BSI) dalam penelitian ini menyediakan contoh konkret dari Cyber Dependent Terrorism. Penelitian ini juga menyoroti bahwa parameter utama dalam mengevaluasi cyberterrorism bukanlah pada korban jiwa atau kerusakan fisik yang langsung tampak, melainkan lebih pada kerusakan data dan dampak psikologis yang diakibatkannya. Dampak serangan siber ini tidak hanya mengganggu layanan publik dan ekonomi, tetapi juga menimbulkan rasa takut dan ketidakamanan di masyarakat. Studi ini menekankan pentingnya pengembangan strategi pencegahan dan respons yang cepat dan efektif dalam menghadapi cyberterrorism, yang meliputi aspek kerjasama internasional dan peningkatan kesadaran serta pendidikan masyarakat. Dengan menggarisbawahi bahwa potensi ancaman cyberterrorism di Indonesia akan terus meningkat, penelitian ini mengajukan pendekatan holistik dalam mengatasi tantangan ini. Pendekatan tersebut mencakup perlunya kebijakan yang lebih kuat, kerjasama antar-sektor yang lebih intensif, dan pengembangan program pendidikan yang bertujuan untuk meningkatkan kesadaran tentang bahaya cyberterrorism. Diharapkan, dengan strategi dan langkah-langkah yang komprehensif ini, Indonesia dapat lebih efektif dalam melindungi keamanan nasionalnya serta privasi dan keamanan warganya dari ancaman cyberterrorism yang berkembang.
.....This paper examines the concept of cyberterrorism in the context of Indonesia, using theoretical approaches developed by Correia (2022) and Prof. Golose (2015), and based on actual cases of cyber attacks in the country. The study focuses on the unique characteristics of cyberterrorism, which include cognitive aspects, where damage in the cyber realm, victims, and the threats posed become important criteria in classifying the type of attack. Correia identifies that cyberterrorism encompasses cyber activities that advocate certain ideologies and threaten the public and property. The analysis of cases such as Bjorka, Polrileak, and the data breach of Bank Syariah Indonesia (BSI) in this study provides concrete examples of Cyber Dependent Terrorism. This paper also highlights that the main parameters in evaluating cyberterrorism are not based on casualties or immediate physical damage, but rather on data damage and the psychological impact it causes. The impact of these cyber attacks disrupts public services and the economy, and also generates fear and insecurity in society. The study emphasizes the importance of developing prevention strategies and rapid and effective responses to cyberterrorism, which include aspects of international cooperation and enhancing public awareness and education. By underlining that the potential threat of cyberterrorism in Indonesia will continue to increase, this study proposes a holistic approach to

address this challenge. This approach includes the need for stronger policies, more intensive inter-sector cooperation, and the development of educational programs aimed at raising awareness of the dangers of cyberterrorism. It is hoped that with these comprehensive strategies and measures, Indonesia can be more effective in protecting its national security as well as the privacy and safety of its citizens from the growing threat of cyberterrorism.