Analisis Ancaman Kejahatan Siber bagi Keamanan Nasional pada Masa Pandemi COVID-19 = Threat Analysis of Cyber Crime for National Security in COVID-19 Pandemic

Abdul Hanief Amarullah, author

Abstrak

COVID-19 adalah varian pneumonia baru yang memiliki kemampuan penyebaran yang sangat cepat. Dampak yang dihasilkan akibat penyebaran virus ini dihadapi di seluruh bagian di dunia. Salah satunya adalah perubahan perilaku dimana kegiatan tatap muka diadakan secara daring, yang berimbas pada peningkatan penggunaan internet dan ruang siber yang disertai dengan peningkatan ancaman kejahatan siber. Penelitian ini bertujuan untuk mengetahui tingkat ancaman kejahatan siber yang terjadi selama masa pandemic COVID-19, serta peran pemerintah dalam mengidentifikasi dan memitigasinya. Data mengenai kejahatan siber dan peristiwa penting yang digunakan merupakan data pada bulan Februari hingga April 2020 dan didapatkan dari berbagai sumber terbuka. Analisa linimasa digunakan terhadap data kejahatan siber dan peristiwa penting sebelum dilakukan analisa terhadap tingkat ancamannya. Kejahatan siber yang terjadi selama masa pandemic dapat dikategorikan ke dalam 4 (empat) agen ancaman yaitu malware, penipuan online, Zoombombing, dan Distributed Denial-of-Service (DDoS). Malware menjadi mayoritas agen ancaman dengan tingkat ancaman ‘kritis’, sementara penipuan online dan DDoS termasuk dalam kategori tingkat ancaman ‘tinggi’ dan zoombombing termasuk dalam kategori tingkat ancaman ‘dapat diabaikan’. Lembaga pemerintah yang bertanggung jawab dalam melakukan deteksi dan mitigasi ancaman kejahatan siber adalah Badan Siber dan Sandi Negara, Badan Intelijen Negara, serta Kepolisian Repiblik Indonesia.

.....COVID-19, a new variant of pneumonia had the ability to spread rapidly. The resulting impact of the rapid spread of the virus can be seen in all parts of the world. One of them is the change of behavior where face-to-face activities are now held online, which has an impact on the increase of internet usage, also the increase of cybercrime threats. This research aims to determine the level of threat of cybercrime that occurred during the COVID-19 pandemic, as well as the role of the Indonesian government in identifying and mitigating it. Data on cybercrime and key events used is data from February through April of 2020, obtained from various open sources. Timeline analysis is used on cybercrime and key events data to help make identifying cybercrime easier before a threat analysis is performed. Cybercrimes that occur during time of research can be categorized into 4 (four) threat agents; malware, online fraud, Zoombombing, and Distributed Denial-of-Service (DDoS). Malware becomes the majority of threat agent, and after the threat analysis is performed, belongs to ‘critical’ level, while online fraud and DDoS fall into the ‘high’ level and zoombombing falls into ‘negligible’ level. Government agencies responsible for detecting and mitigating cyber crime threats are the National Cyber and Crypto Agency, State Intelligence Agency, and Indonesian National Police.