

Ragam ancaman siber dan respon negara dalam menghadapinya = Types of cyber threat and states responses in dealing with them

Elsa Safira Hestriana, author

Deskripsi Lengkap: <https://lib.ui.ac.id/detail?id=20459534&lokasi=lokal>

Abstrak

ABSTRAK

Keamanan siber merupakan isu yang relatif masih baru dalam Ilmu Hubungan Internasional, dan pembahasannya sedang ramai dikembangkan baik oleh akademisi maupun praktisi. Dalam ranah akademik, belum banyak kajian yang meninjau isu ini dalam tataran strategis. Tinjauan pustaka ini bertujuan untuk melihat bagaimana negara-negara membentuk strategi keamanan sibernya. Tulisan ini akan meninjau hal tersebut melalui kategorisasi manifestasi strategi keamanan siber sebagaimana dijelaskan oleh para akademisi dalam literatur tentang keamanan siber. Dengan demikian, tulisan ini akan mengelompokkan negara-negara berdasarkan persepsi aktor ancamannya serta berdasarkan bentuk strategi yang dilakukan. Tulisan ini menemukan dua kesimpulan utama. Pertama, perlindungan infrastruktur merupakan hal utama dari tanggapan negara terhadap keamanan siber secara keseluruhan. Kedua, pembentukan persepsi ancaman siber dan strategi untuk menanggapi masih cenderung bersifat tradisional.

<hr>

ABSTRACT

Cybersecurity is a relatively new issue in International Relations, and the discussion is currently being developed by both scholars and practitioners. There are still limited numbers of study that talk about this issue at the strategic level in the academic fashion. This literature review aims to see how states form their cybersecurity strategies. This paper will observe this through the categorization of cybersecurity strategy manifestations as explained by scholars in literature about cybersecurity. Therefore, this paper will group states based on their perceptions regarding actors that pose cyber threats and the forms of strategy that they perform to respond. This paper finds two main conclusions. First, the protection of infrastructure is the most prominent issue in states response towards cybersecurity. Second, the determination of threat perceptions and forms of strategy to respond cybersecurity still tend to be traditional.