# Sekuritisasi Ruang Siber dalam Hubungan Internasional = The Securitization of Cyberspace in International Relations

Faris Abdurrahman, author



---

Abstrak

Hubungan Internasional merupakan studi yang mencakup dinamika antarnegara, termasuk area penting keamanan siber di era digital. Serangan siber di Estonia dan Iran telah menyoroti ketidaksiapan global dalam menghadapi ancaman siber, mendorong negara-negara untuk mengambil langkah pengamanan dan terlibat dalam diplomasi digital. Kajian ini mengeksplorasi konteks dan variabel pendorong di balik sekuritisasi ruang siber, evolusi norma siber global, serta dinamika pengamanan ruang siber dalam wujud sekuritisasi yang dilakukan. Literatur mengidentifikasi empat mekanisme sekuritisasi—aktor sekuritisasi, speech act, audiens, dan facilitating conditions, sekaligus empat komponen utama keamanan ruang siber—referent object, emergency situations, existential threat, dan extraordinary measures. Kemajuan pesat teknologi informasi dan komunikasi (TIK) telah mengubah lanskap keamanan global, yang menuntut kebijakan keamanan siber yang adaptif. Akibatnya, fokus telah bergeser dari hanya melindungi infrastruktur menjadi memahami operasi siber, menempatkan ruang siber sebagai elemen penting dalam strategi keamanan nasional. Pendekatan extraordinary measures seperti multistakeholderisme dan kedaulatan digital menekankan kolaborasi antar pemangku kepentingan dan kontrol negara yang kuat. Eksplorasi strategi keamanan siber mencakup tindakan pencegahan dan mitigasi, potensi jalur kerjasama, dan formulasi kebijakan yang efektif. Kajian ini menekankan kebutuhan pendekatan holistik dan kooperatif terhadap sekuritisasi ruang siber, memberikan wawasan yang dapat diterapkan pada wilayah lain yang menghadapi tantangan serupa dan mewakili jalan yang menjanjikan untuk penelitian di masa depan.
..... International Relations encompasses the dynamics between nations, including the critical area of cybersecurity in the digital era. Recent cyberattacks on Estonia and Iran have highlighted global unpreparedness in addressing cyber threats, prompting nations to establish control measures and engage in digital diplomacy. This analysis explores the context and driving variables behind the securitization of cyberspace, along with the evolution of global cyber norms and the dynamics of cyber security through the lens of securitization. Literature identifies four mechanisms of securitization—securitizing actors, speech acts, the audience, and facilitating conditions, as well as four main components of cybersecurity—referent objects, emergency situations, and existential threats. The rapid advancement of information and communication technology (ICT) has transformed the global security landscape, necessitating adaptive cybersecurity policies. Consequently, the focus has shifted from safeguarding infrastructure to understanding cyber operations, positioning cyberspace as crucial in national security strategies. Extraordinary measure approaches such as multistakeholderism and digital sovereignty emphasize collaboration among stakeholders and robust state control. The exploration of cybersecurity strategies includes preventive and mitigation actions, potential cooperation avenues, and effective policy formulation. This analysis underscores the need for a holistic and cooperative approach to the securitization of cyberspace, providing insights applicable to other regions facing similar challenges and representing a promising avenue for future research.