

Anticipatory Self-Defense in Cyber Contexts: Assessing Its Lawfulness and Applicability in International Law

QueeneY Fionnula Easter Sutanto, Fajri Matahati Muhammadin, S.H., LL.M., Ph.D.

ABSTRACT

The increasing prevalence of cyberattacks poses significant challenges to traditional concepts of self-defense under international law, requiring states to navigate an evolving digital battlefield that transcends borders. Cyber threats, characterized by speed, anonymity, and their potential to cause widespread disruption to critical infrastructure, necessitate a reevaluation of anticipatory self-defense principles. This research investigates the conditions under which cyber operations can qualify as armed attacks or imminent threats, justifying preemptive defensive measures in accordance with the UN Charter, Tallinn Manual, and the Caroline doctrine. Using a normative legal approach, the study analyzes key legal concepts such as attribution, imminence, necessity, and proportionality, which are essential in determining the legality of ASD in cyberspace. Through case studies from both developed and developing countries—including Indonesia, Kenya, Bangladesh, the United States, Iran, Israel, and Russia—this research highlights the global nature of cyber threats and the varying challenges faced by different nations. These incidents demonstrate that, despite differences in technical capacity and legal frameworks, no state is immune to the growing threat posed by cyberattacks. The study further argues that existing international frameworks must evolve to address gaps in accountability, particularly in enhancing attribution mechanisms and refining the concept of imminence in the cyber domain. Achieving a global consensus on cybersecurity is critical to ensure states can take lawful preemptive actions while upholding the principles of international peace, sovereignty, and security in an increasingly digital world.

Keywords: Anticipatory Self-Defense, Cyberattacks, Cyberlaw, *jus ad bellum*.

Anticipatory Self-Defense in Cyber Contexts: Assessing Its Lawfulness and Applicability in International Law

Queeney Fionnula Easter Sutanto, Fajri Matahati Muhammadin, S.H., LL.M., Ph.D.

INTISARI

Meningkatnya serangan siber menimbulkan tantangan signifikan terhadap konsep tradisional pembelaan diri dalam hukum internasional, yang memaksa negara-negara untuk menavigasi medan perang digital yang terus berkembang dan melintasi batas-batas wilayah. Ancaman siber yang ditandai dengan kecepatan, anonimitas, serta potensinya untuk menyebabkan gangguan luas terhadap infrastruktur kritis, memerlukan evaluasi ulang terhadap prinsip anticipatory self-defense. Penelitian ini mengkaji kondisi di mana operasi siber dapat diklasifikasikan sebagai serangan bersenjata atau ancaman yang akan segera terjadi, yang membenarkan tindakan defensif preemptif sesuai dengan Piagam PBB, Tallinn Manual, dan doktrin Caroline. Dengan pendekatan analisis hukum normatif, studi ini membahas konsep hukum kunci seperti atribusi, kedaruratan, kebutuhan, dan proporsionalitas yang penting dalam menentukan legalitas ASD di ruang siber. Melalui studi kasus dari negara maju dan berkembang—termasuk Indonesia, Kenya, Bangladesh, Amerika Serikat, Iran, Israel, dan Rusia—penelitian ini menyoroti sifat global dari ancaman siber dan tantangan yang dihadapi oleh berbagai negara. Insiden-insiden ini menunjukkan bahwa, meskipun terdapat perbedaan dalam kapasitas teknis dan kerangka hukum, tidak ada negara yang kebal terhadap ancaman serangan siber yang semakin meningkat. Studi ini juga berpendapat bahwa kerangka kerja internasional yang ada harus berkembang untuk mengatasi kekosongan dalam akuntabilitas, terutama dalam meningkatkan mekanisme atribusi dan memperbaiki konsep kedaruratan di domain siber. Mencapai konsensus global tentang keamanan siber sangat penting untuk memastikan bahwa negara dapat mengambil tindakan preemptif yang sah sambil menjunjung tinggi prinsip perdamaian, kedaulatan, dan keamanan internasional dalam dunia yang semakin digital.

Kata Kunci: Anticipatory Self-Defense, Cyberattacks, Cyberlaw, *jus ad bellum*.