International Journal of Society Reviews (INJOSER) https://injoqast.net/index.php/INJOSER
Vol. 3 No. 11 2026, pages: 266~272 e-ISSN: 3030-802X

INTERNATIONAL LEGAL FRAMEWORKS FOR ADDRESSING CROSS-BORDER CYBERCRIME AND DIGITAL SECURITY THREATS

Aliffia Fahrani
Law Study Program, Faculty of Law, Warmadewa University
E-mail : aliffiafahranialiffia@gmail.com[1]

ABSTRACT

This article analyzes the effectiveness of international legal frameworks in addressing cross-border cybercrime and digital security threats. The rapid development of digital technology has increased the complexity of cybercrime, which transcends national borders and challenges traditional principles of territorial jurisdiction. This study employs a normative legal research method using statutory and conceptual approaches, with analysis of primary legal instruments such as the Budapest Convention on Cybercrime (2001) and United Nations initiatives on cybercrime governance, as well as relevant national legislation in Indonesia. The findings indicate that international legal frameworks provide an important normative foundation for cybercrime regulation; however, their effectiveness remains limited due to fragmented implementation, lack of universal participation, jurisdictional complexity, and regulatory lag in responding to technological developments. Cybercriminals exploit these legal gaps, creating enforcement challenges across jurisdictions. In addition, Indonesia faces structural constraints in cybercrime enforcement, particularly in digital forensic capacity and cross-border cooperation mechanisms. This study concludes that although existing international legal frameworks are normatively adequate, their practical effectiveness is still constrained. Therefore, stronger legal harmonization, enhanced international cooperation, and adaptive regulatory mechanisms are required to address the evolving nature of cybercrime and digital security threats.

Keywords: cybercrime, international law, jurisdiction, digital security, legal harmonization

INTRODUCTION

The rapid expansion of digital technology has fundamentally transformed global interaction, economic systems, and governance structures. However, alongside these advancements, cybercrime has emerged as a persistent transnational threat that transcends territorial boundaries and challenges traditional legal doctrines. Cybercrime activities such as unauthorized access, ransomware attacks, identity theft, online financial fraud, and cyber espionage increasingly involve actors operating across multiple jurisdictions, making enforcement significantly more complex (Wall, 2017; Brenner, 2019).

One of the core legal challenges in addressing cybercrime is its borderless nature, which undermines the applicability of classical principles of territorial jurisdiction. In traditional international law, state sovereignty determines the scope of legal authority; however, cyberspace disrupts this structure by enabling perpetrators to operate remotely from jurisdictions where enforcement may be weak or non-cooperative (Chang, 2020). As a result, cybercriminals often exploit legal asymmetries between states, creating enforcement gaps and safe havens that hinder prosecution efforts (UNODC, 2022).