

23 - 25 October 2026

Geneva , Switzerland

Transnational Cybercrime and the Inadequacy of International Criminal Law Mechanisms

Dr. Ștefănoaia Mihai*Ștefan cel Mare University, Suceava, Romania*

Abstract

The rapid expansion of digital technologies has transformed cybercrime into an increasingly transnational phenomenon that challenges traditional models of criminal jurisdiction and international cooperation. Cyberattacks, ransomware, online fraud, identity theft, and attacks against critical infrastructure may involve perpetrators, victims, servers, and digital evidence located simultaneously across multiple jurisdictions. This paper examines the extent to which existing international criminal law and cooperation mechanisms are capable of responding effectively to the cross-border nature of cybercrime. Particular attention is given to jurisdictional fragmentation, conflicts of jurisdiction, difficulties in attribution, disparities between national criminal laws, and obstacles affecting the collection and transfer of electronic evidence. The study adopts a legal and comparative approach, examining relevant international instruments and mechanisms of judicial and law-enforcement cooperation. It argues that, despite significant developments in international cooperation, the current framework remains fragmented and largely dependent on domestic criminal justice systems, creating enforcement gaps that may be exploited by cybercriminal networks. The paper therefore considers the need for stronger harmonization of substantive and procedural rules, more efficient mechanisms for cross-border access to digital evidence, and enhanced international cooperation. It concludes that an effective response to transnational cybercrime requires a coordinated legal framework capable of reconciling enforcement effectiveness with jurisdictional sovereignty and fundamental rights.

Keywords: Transnational Cybercrime; International Criminal Law; Cybercrime Jurisdiction; Digital Evidence; International Cooperation; Criminal Liability; Cybersecurity.