7. Garcia, Frank. “Open Regionalism and Its Role in Digital Trade” / Frank Garcia // International Law Review. – Vol. 30. – №. 2. – 2019. – P. 90–115.

8. Zhao, Lin. “Lex Mercatoria in the Digital Age: The Evolution of Digital Trade Norms” / Lin Zhao // Global Trade Studies. – Vol. 27. – № 1. – 2023. – P. 14–38.

9. Chander, Anupam. “Digital Trade and the USMCA: Enforceability and Beyond” / Anupam Chander, Uyen Le // North American Trade Journal. – Vol. 22. – № 1. – 2021. – P. 78–102.

On the issue of legal regulation of cyberspace from the point of view of international law

Zhu He, postgraduate student, BSU,
supervisor Merkushin V. V., PhD (law), docent

The governance of cyberspace under contemporary international law faces unprecedented challenges, balancing state sovereignty, cybersecurity imperatives, and human rights protections. This article analyzes these tensions through the lens of evolving legal norms and state practices, proposing a hybrid governance model that integrates multilateral cooperation with adaptive frameworks. Key case studies – Including the Tallinn Manual, GDPR, and UN initiatives – highlight both progress and gaps in addressing transnational cyber threats [1]. Recommendations emphasize institutionalized accountability, human rights safeguards, and cross-border collaboration to reconcile territorial sovereignty with digital interdependence.

The principle of state sovereignty, central to the UN Charter, faces ambiguity in cyberspace. While states claim control over domestic digital infrastructure (e. g., China’s data localization laws), cross-border data flows challenge exclusive jurisdiction. The “Tallinn Manual 2.0” posits that cyber operations violating territorial integrity breach sovereignty, yet debates persist over non-kinetic actions like data exfiltration [2].

For instance, the 2020 Solar Winds hack exposed the lack of consensus on attributing state responsibility. This incident underscores the need for clearer thresholds under international law to distinguish espionage from acts of aggression under Article 51 of the UN Charter.

Cybersecurity frameworks, such as the Budapest Convention, prioritize protecting critical infrastructure but risk enabling surveillance overreach. China’s 2017 Cybersecurity Law mandates data localization, yet conflicts with privacy rights under the GDPR. Conversely, the EU’s GDPR exemplifies robust data protection but faces extraterritorial enforcement challenges, as seen in “Google v. CNIL” (2019), where the EU Court limited the “right to be forgotten” to regional domains [3]. These tensions reveal a fragmented legal landscape where security measures often undermine universal rights.

Cybercrimes like ransomware attacks (e.g., Colonial Pipeline, 2021) exploit jurisdictional disparities. The absence of a universal treaty allows states to adopt divergent definitions and penalties. While the 2021 UN OEWG report affirms international law's applicability to cyberspace, its non-binding nature limits enforcement. Hybrid mechanisms, such as INTERPOL's Global Cybercrime Program, remain hindered by uneven state cooperation [4].

Thus, cyberspace, as the fifth domain of global interaction, disrupts traditional legal paradigms rooted in territoriality. States grapple with asserting sovereignty over borderless digital infrastructures while combating cyberattacks, data exploitation, and AI-driven threats.

International law can adapt to govern cyberspace effectively, focusing on three pillars: sovereignty, security, and rights. By synthesizing legal scholarship, state practices, and institutional responses, it advocates for a dynamic governance framework that balances national interests with global cooperation.

Cyberspace governance demands reimagining sovereignty as adaptive multilateralism. While territorial integrity remains foundational, legal frameworks must evolve to address digital interdependence. By harmonizing security imperatives with human rights and institutionalizing cross-border collaboration, the international community can mitigate risks while unlocking cyberspace's potential. Future research should explore AI governance and the role of non-state actors in shaping norms, ensuring international law remains responsive to technological advancements.

Literature

1. UN Open-Ended Working Group (OEWG) on the security of and in the use of information and communications technologies in 2021–2025 // DigWatch. – URL: https://wp.dig.watch/processes/un-gge (date of access: 25.03.2025).

2. Schmitt, M. N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt. – United States Naval War College, Newport, Rhode Island, 2017. – 500 p.

3. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) // European Union. – URL: http://data.europa.eu/eli/reg/2016/679/oj (date of access: 25.03.2025).

4. Financial and cybercrimes top global police concerns, says new INTERPOL report (19 October 2022) // INTERPOL. – URL: https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report (date of access: 25.03.2025).