PRIVATE INTERNATIONAL LAW MECHANISMS FOR ATTRIBUTING CYBER LIABILITY IN CROSS-BORDER ARBITRATION DISPUTES: LESSONS FOR UZBEKISTAN

Kaibyldaeva Begaim Mukhitovna
Independent Researcher, Tashkent State University of Law
E-mail: begaimkaibyldaeva@gmail.com
https://doi.org/10.5281/zenodo.20605189

Introduction. The rapid expansion of digital commerce and cross-border data flows has generated a new category of transnational disputes that existing legal frameworks were not designed to address. Cyberattacks, data breaches, ransomware incidents, and the unauthorised use of digital assets increasingly give rise to liability claims across multiple jurisdictions simultaneously, confronting arbitral tribunals with fundamental questions of applicable law, jurisdiction, and the attribution of responsibility. For Uzbekistan, a country undergoing comprehensive digital transformation since the adoption of the Digital Uzbekistan-2030 Strategy and deepening its integration into international trade networks, these challenges are both immediate and strategically consequential.

Private international law (PIL) provides the foundational toolkit for resolving conflicts of law in cross-border civil and commercial matters. Yet its classical doctrines, developed for tangible goods and territorial actors, struggle to accommodate the borderless, multi-actor character of cyberspace. The question of which law governs cyber liability, and how responsibility is attributed among states, corporate intermediaries, and individual perpetrators, remains one of the most contested frontiers of contemporary PIL. International arbitration, with its capacity for party autonomy and flexible choice-of-law analysis, has emerged as the preferred forum for resolving high-value cross-border cyber disputes.

This paper analyses the PIL mechanisms available for attributing cyber liability in cross-border arbitration proceedings, examines the principal doctrinal and institutional challenges that those mechanisms face, and derives lessons for the reform of Uzbekistan's legal and regulatory framework governing cyber disputes.

PIL Frameworks for Cyber Liability: Core Doctrines and Jurisdictional Challenges. The attribution of cyber liability under PIL is governed primarily by three doctrinal pillars: the lex loci delicti (law of the place of the tort), the lex loci damni (law of the place where damage occurs), and the principle of party autonomy in the choice of applicable law. The Rome II Regulation of the European Union, which constitutes the most developed regional PIL instrument for non-contractual obligations, adopts the lex loci damni as its general connecting factor under Article 4(1), permitting parties to choose the governing law after the dispute has arisen under Article 14.[1]

Applying these classical doctrines to cyber incidents creates significant difficulties. First, the place of the harmful act is frequently indeterminate: a cyberattack may be launched from servers in one country, routed through intermediary jurisdictions, and cause financial damage in several others simultaneously. The Hague Conference on Private International Law has acknowledged this structural problem in its 2020 Draft Conclusions and Recommendations on Jurisdiction in International Litigation in Civil and Commercial Matters, noting that existing

[1] European Parliament and Council of the EU. (2007). Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II), Arts. 4(1) and 14. Official Journal of the European Union, L 199/40.

connecting factors require substantial adaptation for digital torts.[2] Second, state attribution in the cyber context intersects with public international law rules that are poorly integrated into PIL reasoning. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, though non-binding, represents the most authoritative scholarly codification of state responsibility norms in cyberspace, and its attribution standards are increasingly referenced by arbitral tribunals adjudicating cyber-related investment disputes.

Uzbekistan's national PIL codification is contained in the Civil Code of 1996 (Part Four, Private International Law) and the Law on International Commercial Arbitration of 2006. Neither instrument contains provisions specifically addressing cyber liability or digital torts. This legislative gap stands in contrast to the growing volume of cross-border e-commerce transactions involving Uzbek entities and the escalating frequency of cybersecurity incidents reported across Central Asia.

Attribution of Cyber Liability in International Arbitration: Institutional and Substantive Dimensions. International commercial arbitration has become the dominant forum for resolving cross-border cyber liability disputes, owing to its procedural flexibility, the enforceability of awards under the 1958 New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards across more than 170 states, and the capacity of parties to select arbitrators with specialist expertise in cybersecurity law and digital forensics.[3] The International Chamber of Commerce (ICC), the Singapore International Arbitration Centre (SIAC), and the London Court of International Arbitration (LCIA) have each introduced procedural guidelines and practice notes addressing the evidentiary and jurisdictional particularities of technology-related disputes.

A central substantive challenge in cyber arbitration is the standard of proof required for attribution. Because cyber operations are routinely conducted through obfuscated infrastructure and anonymised networks, claimants frequently rely on circumstantial evidence, technical indicators of compromise, and third-party threat intelligence reports rather than direct documentary proof. Arbitral practice has developed a flexible approach to evidentiary standards, with tribunals applying a balance-of-probabilities threshold and according significant weight to forensic expert testimony. The IBA Rules on the Taking of Evidence in International Arbitration (2020 revision) provide a procedural foundation for managing digital evidence, including provisions on electronic disclosure and the authentication of electronically stored information.[4]

A further dimension concerns the liability of digital intermediaries, including cloud service providers, internet service providers, and cybersecurity vendors. Tribunals have increasingly applied doctrines of comparative fault, vicarious liability, and contractual indemnification to allocate responsibility among multiple parties in complex supply-chain cyber incidents. The UNCITRAL Model Law on Electronic Commerce and the UNCITRAL Model

[2] Hague Conference on Private International Law. (2020). Draft Conclusions and Recommendations on Jurisdiction in International Litigation in Civil and Commercial Matters. HCCH. https://www.hcch.net/en/projects/legislative-projects/jurisdiction

[3] United Nations. (1958). Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention). United Nations Treaty Series, vol. 330, p. 3; Born, G. B. (2021). International commercial arbitration (3rd ed.), pp. 81–95. Kluwer Law International.

[4] International Bar Association. (2020). IBA Rules on the Taking of Evidence in International Arbitration, Arts. 3 and 9. IBA. https://www.ibanet.org/iba-rules-on-the-taking-of-evidence-in-international-arbitration

Law on Electronic Transferable Records provide supplementary frameworks relevant to the governance of electronic contractual relationships implicated in such disputes.

Cybersecurity and Investment Arbitration: Implications for State Responsibility. The intersection of cybersecurity obligations and investment treaty arbitration represents an emerging frontier with particular relevance for Uzbekistan. Bilateral investment treaties (BITs) concluded by Uzbekistan, of which more than fifty are currently in force, impose upon the host state obligations of fair and equitable treatment, full protection and security, and non-discrimination. The full protection and security standard has historically been interpreted to encompass physical security of investments, but investment tribunals are progressively extending its scope to cover cyber threats to investor assets and information systems.[5]

The Tallinn Manual 2.0 articulates a framework of due diligence under which states bear an obligation to ensure that their territory is not knowingly used for internationally wrongful cyber operations. Where a state fails to take reasonable measures to prevent or halt such operations, it may incur international responsibility, which in turn provides a basis for investor claims under applicable BITs. The ICSID tribunal in the landmark Philip Morris v. Uruguay case, while not a cyber dispute, established the principle that host state regulatory conduct must satisfy a minimum standard of rationality; analogous reasoning is being applied in emerging investment arbitration cases involving inadequate state cybersecurity frameworks.

Uzbekistan ratified the ICSID Convention in 1995 and is subject to investor-state dispute settlement clauses in numerous BITs. The country's Cybersecurity Law of 2022 (Law No. ZRU-764) established baseline obligations for critical information infrastructure operators, yet the law does not address the liability of the state towards foreign investors whose digital assets are compromised as a result of inadequate public cybersecurity governance.[6] This lacuna creates material exposure for Uzbekistan in future investor-state arbitrations.

Comparative Lessons and Reform Directions for Uzbekistan. The comparative experience of Singapore and the Netherlands offers instructive models for Uzbekistan. Singapore has integrated cybersecurity obligations into its investment treaty negotiating template, provides mandatory disclosure of cyber incidents affecting listed companies, and has endowed the Singapore International Arbitration Centre with a dedicated Technology, Media and Telecommunications panel of specialist arbitrators. The Netherlands, operating under the EU framework, applies Rome II systematically to cyber tort claims and has developed a well-tested body of case law on the extraterritorial application of data protection obligations under the General Data Protection Regulation (GDPR) to cyber liability in arbitral proceedings.[7]

On the basis of this comparative analysis, the following legislative and institutional reforms are recommended for Uzbekistan. In the legislative sphere, it is necessary to supplement the Private International Law provisions of the Civil Code with specific conflict-of-law rules for non-contractual cyber liability, adopting the lex loci damni as the primary connecting factor whilst preserving party autonomy to designate an alternative law after the

[5] Yannaca-Small, K. (Ed.). (2010). Arbitration under international investment agreements: A guide to the key issues, pp. 312–318. Oxford University Press; UNCTAD. (2024). World Investment Report 2024. United Nations.
[6] Republic of Uzbekistan. (2022). Law on Cybersecurity (No. ZRU-764 of 15 April 2022). Vedomosti Oliy Majlisi.
[7] Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.), Rule 6, pp. 30–43. Cambridge University Press; Tashkent International Arbitration Centre. (2023). Annual Report 2023. https://tiac.uz/

dispute has arisen; to amend the Law on International Commercial Arbitration to incorporate the 2006 amendments to the UNCITRAL Model Law, which introduce provisions on interim measures relevant to preservation of digital evidence; and to accede to the Budapest Convention on Cybercrime of 2001, which provides the principal multilateral framework for cross-border law enforcement cooperation in cyber matters and whose procedural mechanisms are frequently invoked in parallel to arbitral proceedings.

In the institutional sphere, the Tashkent International Arbitration Centre (TIAC) should establish a specialist panel of arbitrators with verified expertise in cybersecurity law, digital forensics, and information technology contracts. TIAC should further adopt procedural rules on electronic evidence that align with the IBA Rules on the Taking of Evidence in International Arbitration (2020) and provide for rapid interim measures to prevent the destruction or alteration of digital evidence. At the inter-agency level, a coordination mechanism between the State Inspectorate for Cybersecurity, the Ministry of Justice, and the Agency for the Development of the Capital Market should be established to ensure coherent state conduct in investor-state arbitrations involving cyber incidents.

Conclusion. The attribution of cyber liability under private international law remains one of the most complex and rapidly evolving areas of transnational legal practice. The classical PIL connecting factors, though adaptable, require targeted legislative modernisation to accommodate the structural features of cyberspace: territorial indeterminacy, multi-actor chains of causation, and the fusion of public and private law dimensions in state-sponsored or state-tolerated cyber operations. For Uzbekistan, the reform of its PIL framework for cyber liability is not merely a technical legal exercise but a strategic investment in the credibility and attractiveness of the national legal system for international business and arbitration users.

The integration of cyber-specific provisions into BITs under negotiation, the modernisation of TIAC's procedural rules, and the alignment of the Cybersecurity Law of 2022 with international attribution standards represent three mutually reinforcing pillars of a coherent national strategy. Future research should examine the specific case law of investment tribunals on the full protection and security standard in the digital environment, as well as the regional harmonisation of cyber PIL norms within the framework of the Shanghai Cooperation Organisation and the Commonwealth of Independent States.

Adabiyotlar, References, Литературы:

1. Born, G. B. (2021). International commercial arbitration (3rd ed.). Kluwer Law International.
2. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention), ETS No. 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
3. European Parliament and Council of the EU. (2007). Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II). Official Journal of the European Union, L 199/40.
4. Hague Conference on Private International Law. (2020). Draft Conclusions and Recommendations on Jurisdiction in International Litigation in Civil and Commercial Matters. HCCH. https://www.hcch.net/en/projects/legislative-projects/jurisdiction
5. International Bar Association. (2020). IBA Rules on the Taking of Evidence in

International Arbitration. IBA. https://www.ibanet.org/iba-rules-on-the-taking-of-evidence-in-international-arbitration

6. Republic of Uzbekistan. (2006). Law on International Commercial Arbitration (No. ZRU-23 of 16 October 2006). Vedomosti Oliy Majlisi.

7. Republic of Uzbekistan. (2022). Law on Cybersecurity (No. ZRU-764 of 15 April 2022). Vedomosti Oliy Majlisi.

8. Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge University Press.

9. Tashkent International Arbitration Centre. (2023). Annual Report 2023. TIAC. https://tiac.uz/

10. UNCTAD. (2024). World Investment Report 2024: Investing in Sustainable Development. United Nations. https://unctad.org/wir2024

11. United Nations Commission on International Trade Law. (2006). UNCITRAL Model Law on International Commercial Arbitration (as amended). United Nations. https://uncitral.un.org/en/texts/arbitration/modellaw/commercial_arbitration

12. United Nations. (1958). Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention). United Nations Treaty Series, vol. 330, p. 3.

13. Yannaca-Small, K. (Ed.). (2010). Arbitration under international investment agreements: A guide to the key issues. Oxford University Press.