E-ISSN: 2997-9439

American Journal of Education and Evaluation Studies
https://semantjournals.org/index.php/_AJEES

| Research Article

Check for updates

Cross-Border Cyber Incidents in International Commercial Arbitration: Private International Law Approaches to Jurisdiction and Applicable Law

Kaibyldaeva Begaim Mukhitovna
Independent Researcher, Tashkent State University of Law
E-mail: begaimkaibyldaeva@gmail.com

Abstract: This article examines the private international law (PIL) challenges arising from cross-border cyber incidents in the context of international commercial arbitration. As commercial transactions increasingly rely on digital infrastructure, disputes involving ransomware attacks, data breaches, cyber fraud, and electronic contract manipulation have proliferated, generating complex questions of arbitral jurisdiction and applicable law. The article analyses three interlocking issues: first, the determination of arbitral jurisdiction over multi-party and multi-contract cyber disputes; second, the identification of the law applicable to cyber-related claims under leading PIL instruments, including the Rome I and Rome II Regulations, the UNCITRAL Model Law, and common law frameworks; and third, the recognition and enforcement of arbitral awards involving cyber incidents under the 1958 New York Convention. Special attention is given to the tension between territorially anchored PIL connecting factors and the inherently borderless nature of cyberspace. The article concludes that existing PIL frameworks require purposive adaptation to address the specificities of cyber incidents, and proposes a set of principles for choice-of-law clauses and procedural orders designed to reduce legal uncertainty in cyber-related international arbitration.

Keywords: Private International Law, Cross-Border Cyber Incidents, International Commercial Arbitration, Applicable Law, Jurisdiction, New York Convention, Rome II Regulation, Cybersecurity, Lex Loci Damni, Party Autonomy, Choice-of-Law, Cyber Fraud

Introduction

The digitisation of international commerce has transformed both the volume and the character of cross-border disputes. Cyber incidents, ranging from targeted ransomware attacks against corporations to large-scale data breaches affecting millions of consumers, are no longer exceptional events but systemic features of the global digital economy [1]. Between 2019 and 2024, reported cyber losses in international commercial transactions exceeded USD 8 trillion annually according to industry estimates, while litigation and arbitration arising from such incidents has multiplied correspondingly. International commercial arbitration, long regarded as the preferred mechanism for resolving transnational commercial disputes, has emerged as a primary forum for adjudicating cyber-related claims, offering the parties the procedural flexibility, confidentiality, and cross-border enforcement that state courts frequently cannot provide [2].

Yet the application of arbitral procedures to cyber disputes raises a distinct set of challenges that existing legal frameworks were not designed to address. Chief among these challenges are questions of private

international law (PIL): which tribunal has jurisdiction over a dispute involving cyber incidents that occurred across multiple jurisdictions? Which national law governs the contractual and non-contractual obligations arising from a cyber breach? When an arbitral award involving cyber-related claims is rendered, can it be recognised and enforced in a jurisdiction that may characterise cyber-fraud differently from the seat of arbitration? These questions sit at the intersection of international arbitration law, conflict of laws, and cybersecurity law, three fields that have developed largely in parallel without adequate cross-pollination [3], [4].

The academic literature on cyber disputes in arbitration has grown substantially in recent years, yet it remains fragmented along disciplinary lines. Arbitration scholars focus predominantly on procedural cybersecurity, that is, on protecting the arbitral process itself from cyber intrusion, rather than on the substantive PIL questions that arise when the dispute is about a cyber incident. Conflict-of-laws scholars, conversely, have engaged with cyber torts mainly in the context of state court litigation under instruments such as the Rome II Regulation, the Restatement (Third) of Conflict of Laws, or the Hague Principles on Choice of Law in International Commercial Contracts, without systematically addressing the peculiarities of arbitration. The present article aims to bridge this gap through an integrated doctrinal analysis of PIL approaches to jurisdiction and applicable law in cross-border cyber arbitration [5].

Cross-Border Cyber Incidents as Objects of International Commercial Arbitration. The first preliminary question is whether cyber incidents fall within the subject-matter scope of international commercial arbitration. Three categories of cyber incidents recurrently generate arbitral proceedings in international commerce. The first is contractual cyber breach: a party to an international commercial contract fails to implement agreed cybersecurity measures, resulting in a data breach or system compromise that causes economic loss to the counterparty [6]. Such claims are straightforwardly contractual in character and have been submitted to arbitration under standard dispute resolution clauses in technology service agreements, data processing agreements, and supply chain contracts. The second category is cyber-enabled fraud: a third-party attacker compromises email systems or payment platforms to intercept and redirect commercial communications, leading to fraudulent transfers. These cases generate mixed contractual and tortious claims involving multiple parties across different jurisdictions. The third category is ransomware disruption: an attack renders a party unable to perform contractual obligations, raising force majeure defences, business interruption claims, and potential liability of cybersecurity service providers [7].

The arbitrability of such disputes under the lex arbitri, that is, the law of the seat of arbitration, is generally not in doubt when the claims arise from a commercial contract containing a valid arbitration clause. The more contentious questions arise with respect to non-contractual claims. In several jurisdictions, courts have held that tortious claims arising from the same transaction as a contractual relationship may be swept within the scope of a broadly drafted arbitration clause under the doctrine of close connection [8]. The 2021 ICC Arbitration Rules address the procedural dimension of multi-party cyber disputes by permitting joinder of additional parties and consolidation of related arbitrations, which is particularly relevant when a single cyber incident generates claims involving multiple contracts.

Methodology

Jurisdictional Challenges: Arbitral Jurisdiction over Multi-Jurisdictional Cyber Disputes. Arbitral jurisdiction over cross-border cyber disputes raises at least three distinct analytical problems. The first is the temporal problem: cyber incidents are often discovered long after they occurred, and the arbitration clause may have been contained in an agreement executed before the relevant digital systems were put in place, raising questions of ratione temporis scope. The second is the geographical problem: a single cyber incident may originate from a server in one jurisdiction, transit network infrastructure in several others, cause harm in

yet another, and implicate data of individuals located across the globe. The third is the party problem: the direct contractual counterparties may not be the only persons affected by the incident; third-party data subjects, subcontractors, and insurers may all seek to pursue claims, yet their access to arbitration depends on whether they can be characterised as parties to the arbitration agreement.

With respect to the geographical problem, traditional PIL doctrine developed the connecting factor of the lex loci delicti as the primary determinant of jurisdiction and applicable law in tort. When applied to cyber incidents, this factor becomes almost entirely arbitrary: the place where the harmful act was performed may be the server farm of a hosting provider that bears no meaningful connection to either party, while the place where the harm manifested may be a bank in a third state. American courts have responded to this difficulty by developing a purposive effects test, asking in which jurisdiction the plaintiff was primarily targeted and suffered the most significant injury. European courts have applied Article 7(2) of the Brussels I bis Regulation, which confers jurisdiction on both the court of the place of the harmful event and the court of the place of the resulting damage, producing parallel proceedings across multiple EU member states in cases of multi-jurisdictional cyber attacks.

International arbitration offers a structural advantage over state court litigation in this respect. An arbitration agreement properly construed can vest a single tribunal with jurisdiction over all claims arising from a cyber incident, regardless of where the act or its effects occurred. The seat of arbitration, typically chosen by the parties in advance, provides a stable territorial anchor for supervisory court jurisdiction without requiring the parties to litigate the locus delicti question. Moreover, under Article II of the New York Convention, arbitration agreements must be recognised by contracting states and given effect in preference to national jurisdictional rules, meaning that a validly concluded arbitration clause generally precludes competing proceedings in state courts.

Results and Discussion

Nevertheless, the extension of arbitral jurisdiction to third parties affected by a cyber incident remains problematic. The doctrine of non-signatories to arbitration agreements has been addressed in leading arbitral rules and domestic arbitration laws, but its application to cyber disputes is unsettled. A subcontractor who processes data on behalf of the main contractor may not be a signatory to the arbitration agreement between the principal parties, yet its conduct may be central to the cybersecurity breach [9]. Several tribunals have extended jurisdiction over non-signatories on the basis of group of companies doctrine, implied consent, or equitable estoppel, but these approaches remain controversial and are not uniformly accepted across jurisdictions.

Applicable Law for Contractual Cyber Claims: Party Autonomy and Its Limits. For contractual cyber claims, the point of departure in virtually all PIL systems is the principle of party autonomy: parties to an international commercial agreement are free to designate the law governing their contract, including any disputes arising from cyber incidents. This principle is enshrined in Article 3 of the Rome I Regulation, Article 6 of the Hague Principles on Choice of Law in International Commercial Contracts, and the domestic conflict-of-laws rules of most commercially significant jurisdictions [10]. In the arbitration context, party autonomy is reinforced by the lex arbitri: most arbitration laws permit the tribunal to apply the law chosen by the parties, and only in the absence of such choice does the tribunal apply the PIL rules of the seat or those it considers most appropriate.

However, party autonomy in cyber-related contracts faces two significant constraints. The first is the operation of overriding mandatory rules. In the European context, data protection obligations under the General Data Protection Regulation (GDPR) are mandatory rules in the sense of Article 9 of Rome I: they apply regardless of the choice of governing law, and an arbitral award that contravenes GDPR

requirements may be refused enforcement in EU member states on public policy grounds [11]. This creates a layer of regulatory compliance that supervenes the parties' contractual choices and must be considered by any tribunal adjudicating cyber claims involving EU-established parties or EU-resident data subjects. The second constraint is the phenomenon of dépeçage, the splitting of applicable law across different issues in a dispute. A cyber incident involving a data breach may give rise simultaneously to contractual claims governed by the chosen law, non-contractual claims governed by the lex loci damni, and regulatory claims governed by mandatory rules of the jurisdiction where the data processing occurred. Managing this plurality of applicable laws requires careful procedural organisation and is one of the primary sources of complexity in cyber arbitration [12].

Absent an express choice of law, the arbitral tribunal must identify the governing law through PIL rules. In practice, most international arbitral tribunals operating under institutional rules apply either the PIL rules of the seat or the conflict-of-laws method they consider most appropriate, with a strong tendency toward the latter approach under rules such as Article 21(1) of the ICC Rules and Article 22(3) of the LCIA Rules. For cyber-related contractual disputes, the most significant relationship test of the Restatement (Third) of Conflict of Laws and the characteristic performance test of Article 4 of Rome I both point toward the law of the party that is required to implement and maintain the cybersecurity obligations, typically the technology service provider or data processor [13]. This result accords with the reasonable expectations of the parties and provides a measure of predictability.

Applicable Law for Non-Contractual Cyber Claims: The Lex Loci Damni and Its Discontents. The most contested area of PIL in cross-border cyber disputes concerns non-contractual claims, that is, claims in tort, delict, or unjust enrichment arising from a cyber incident independently of any contractual relationship. The paradigmatic case is a cyber attack by a third-party threat actor who compromises the digital infrastructure of a commercial enterprise, causing financial loss to the enterprise and its trading partners. The injured parties may have no contractual relationship with the attacker, and their claims must therefore be framed in tort.

Under Article 4 of the Rome II Regulation, the general rule for tort is the lex loci damni: the law of the country in which the direct damage occurred, irrespective of the country in which the indirect consequences of that event occur. Applied to cyber torts, this rule generates notorious difficulties. Financial damage from a cyber incident may manifest in multiple countries simultaneously: a company headquartered in Germany, with bank accounts in Switzerland, trading in US dollars, may suffer financial loss in each of those jurisdictions depending on which legal system's conception of damage is applied. The Court of Justice of the European Union has held, in the context of online defamation and data breaches, that courts may apply a mosaic approach, restricting each national court to the damage suffered in its territory, but this approach is ill-suited to arbitration, which is expected to resolve the entire dispute in a single proceeding [14].

An alternative approach, adopted by certain arbitral tribunals and academic commentators, is to identify a single most-connected law for the entire cyber tort. This approach draws on the flexibility afforded to arbitral tribunals by institutional rules, which typically permit the tribunal to apply the conflict-of-laws rule it considers appropriate. Factors relevant to identifying the most-connected law for a cyber tort include: the location of the targeted systems; the residence of the entity responsible for maintaining those systems; the market in which the commercial activity was conducted; and the place where the injury was felt most acutely. This functional approach is consistent with both the Restatement (Third) of Conflict of Laws and the traditional English choice-of-law methodology, and has the practical advantage of producing a single governing law for the non-contractual aspects of the dispute.

An important PIL mechanism that can reduce conflicts of applicable laws is the escape clause. Article 4(3)

of Rome II allows departure from the lex loci damni rule where it is clear from all the circumstances that the tort is manifestly more closely connected with another country. For cyber torts involving parties who are already in a contractual relationship, this clause often leads to the application of the law governing the contract, producing a more coherent and predictable legal framework. Arbitral tribunals have drawn on an analogous principle, treating the law of the underlying commercial relationship as an implicit choice-of-law for non-contractual claims arising from the same transaction, unless the parties have evidenced a contrary intention.

Recognition and Enforcement of Arbitral Awards in Cyber Disputes. The recognition and enforcement of arbitral awards involving cyber incidents under the New York Convention raises two principal PIL issues: the public policy exception under Article V(2)(b) and the due process exception under Article V(1)(b). Both exceptions have been invoked, with varying degrees of success, in the context of arbitrations where the manner in which the proceedings were conducted, or the substance of the award, was alleged to have violated fundamental legal norms of the enforcing state.

The public policy exception is most likely to be invoked where an award in a cyber dispute conflicts with the mandatory data protection law of the enforcing state. In EU member states, an award that requires a party to disclose data in violation of the GDPR, or that awards damages calculated on a basis inconsistent with GDPR principles of accountability, may be subject to challenge on public policy grounds. Courts in France, Germany, and the Netherlands have all recognised that data protection rules constitute a fundamental principle of the legal order capable of engaging the public policy exception, although they have generally applied this exception narrowly and refused enforcement only in cases of manifest incompatibility. This cautious approach reflects the pro-enforcement bias of the New York Convention and the general principle that the public policy exception should not be used as a pretext for reviewing the merits of an award.

The due process exception under Article V(1)(b) is particularly relevant to cyber disputes because a cyber attack on the arbitral proceedings themselves, for example through interception of communications or tampering with electronic evidence, could give rise to a denial of the opportunity to present one's case. The UK Supreme Court in Dallah v. Pakistan confirmed that due process requirements under the New York Convention are of fundamental importance and any serious procedural irregularity may justify refusal of enforcement. While that case did not involve a cyber incident, its reasoning applies with equal force to situations where a party's ability to participate fully in the arbitration was compromised by a cybersecurity breach, whether caused by the opposing party, a third-party attacker, or the inadequacy of the institution's digital infrastructure [15].

A further enforcement issue concerns the recognition of arbitral awards involving claims that a national court in the enforcing state characterises as non-arbitrable. In certain jurisdictions, claims involving personal data breaches or privacy violations have been treated as matters of public law that fall outside the scope of arbitration. While this position is inconsistent with the broad conception of commercial arbitrability that prevails in major arbitration centres, it may operate as an obstacle to enforcement in states with restrictive arbitrability rules [16], [17]. Drafters of international commercial contracts should accordingly be attentive to the arbitrability rules of all jurisdictions in which enforcement may be sought, not only the law of the seat.

Emerging Frameworks and Reform Proposals. The inadequacy of existing PIL frameworks to address cross-border cyber incidents in arbitration has prompted a range of reform initiatives at the institutional, national, and international levels. At the institutional level, the ICCA-ICC Cybersecurity Protocol has established a set of baseline principles for the protection of the arbitral process from cyber intrusion, including requirements for information security assessments, encryption of communications, and secure storage of

evidence. While the Protocol primarily addresses procedural cybersecurity rather than PIL, its adoption as a contractual term in procedural orders transforms soft-law recommendations into binding obligations, which may in turn affect the PIL analysis of liability for breaches of those obligations [18].

At the national level, several jurisdictions have amended their arbitration statutes to address digital proceedings [19]. Singapore's International Arbitration Act amendments in 2020 extended the powers of tribunals to manage electronic documents and communications. The SIAC Arbitration Rules introduced express provisions on cybersecurity obligations and electronic communications, creating an institutional framework that supplements the parties' choice of law with mandatory procedural standards. These developments suggest a gradual process of normative crystallisation by which soft-law standards for cyber-related arbitration are hardening into binding institutional and legislative rules.

At the international level, UNCITRAL Working Group II has discussed the possibility of developing model contractual clauses for choice of law in cyber-related disputes, building on the framework established by the 2015 UNCITRAL Notes on Online Dispute Resolution [20]. A more ambitious proposal would involve the elaboration of a bespoke international instrument, akin to the Hague Principles on Choice of Law, specifically addressing the PIL aspects of cross-border cyber incidents. Such an instrument could resolve the tension between the lex loci damni rule and the borderless character of cyberspace by introducing a presumptive choice-of-law rule keyed to the residence of the party responsible for the compromised digital infrastructure, subject to displacement in favour of a manifestly more closely connected law [21], [22].

In the absence of such an instrument, practitioners can reduce PIL uncertainty through careful drafting of arbitration agreements and choice-of-law clauses. An effective cyber-oriented choice-of-law clause should, at minimum, designate the law governing the contract; specify the law applicable to non-contractual claims arising from the same digital infrastructure or data processing activities; address the relationship between the chosen law and mandatory data protection rules of potentially affected jurisdictions; and incorporate by reference a recognised cybersecurity protocol such as the ICCA-ICC Cybersecurity Protocol [23]. The choice of arbitral seat should also take account of the data protection and cybercrime laws of the seat jurisdiction, since those laws may operate as mandatory rules affecting both the conduct of the proceedings and the enforceability of the award.

Conclusion

The foregoing analysis leads to several conclusions. First, cross-border cyber incidents generate a genuinely distinct category of PIL challenges in international commercial arbitration, characterised by the multiplicity of potentially applicable laws, the difficulty of applying territorial connecting factors to inherently deterritorialised events, and the interaction between party autonomy and mandatory data protection regimes. Second, international commercial arbitration offers structural advantages over state court litigation for resolving cyber disputes, but those advantages are only fully realised when the arbitration agreement and applicable choice-of-law clause have been carefully drafted to address the specific features of cyber incidents. Third, existing PIL frameworks, including the Rome I and Rome II Regulations, the UNCITRAL Model Law, and the New York Convention, can accommodate cyber disputes through purposive interpretation, but they require adaptation to avoid results that are arbitrary or inconsistent with the parties' reasonable expectations.

Fourth, the public policy and due process exceptions to recognition and enforcement of arbitral awards under the New York Convention have genuine relevance in the cyber context, particularly where data protection mandatory rules are engaged or where the arbitral proceedings themselves were compromised by a cyber incident. Fifth, the emerging soft-law frameworks, notably the ICCA-ICC Cybersecurity Protocol and the cybersecurity provisions of leading institutional rules, represent a significant step toward a

coherent transnational regime for cyber-related arbitration, but their ultimate value depends on their consistent integration into arbitration agreements, procedural orders, and institutional practices.

Further research is needed on at least three fronts: the content and limits of the cyber-security public policy standard for purposes of New York Convention enforcement; the conditions under which non-signatories to arbitration agreements may be subjected to arbitral jurisdiction in multi-party cyber incidents; and the optimal design of choice-of-law clauses for contracts involving significant digital infrastructure and cross-border data processing. The resolution of these questions will require sustained collaboration between international arbitration scholars, PIL specialists, and cybersecurity law experts, reflecting the genuinely interdisciplinary character of the challenges that cross-border cyber incidents pose to the international legal order.

REFERENCES

[1] American Law Institute, *Restatement (Third) of Conflict of Laws*, Tentative Draft No. 4. Philadelphia, PA, USA: ALI Publishers, 2023.

[2] G. B. Born, *International Commercial Arbitration*, 3rd ed., 3 vols. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2021.

[3] *Dallah Real Estate and Tourism Holding Co. v. Ministry of Religious Affairs, Government of Pakistan*, [2010] UKSC 46.

[4] *Dicey, Morris & Collins on the Conflict of Laws*, 16th ed. London, U.K.: Sweet & Maxwell, 2022.

[5] B. Hanotiau, *Complex Arbitrations: Multi-Party, Multi-Contract, Multi-Issue and Class Actions*. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2005.

[6] International Council for Commercial Arbitration (ICCA) and International Chamber of Commerce (ICC), *ICCA-ICC Task Force Report on Cybersecurity in International Arbitration*. The Hague, Netherlands: ICCA, 2022. [Online]. Available: ICCA Official Website

[7] International Bar Association (IBA), *IBA Rules on the Taking of Evidence in International Arbitration*. London, U.K.: IBA, 2020.

[8] International Chamber of Commerce (ICC), *ICC Arbitration Rules (2021 Version)*. Paris, France: ICC Publishing, 2021.

[9] G. Kaufmann-Kohler and T. Schultz, *Online Dispute Resolution: Challenges for Contemporary Justice*. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2004.

[10] J. D. M. Lew, L. A. Mistelis, and S. M. Kroll, *Comparative International Commercial Arbitration*, 2nd ed. Alphen aan den Rijn, The Netherlands: Kluwer Law International, 2021.

[11] London Court of International Arbitration (LCIA), *LCIA Arbitration Rules 2020*. London, U.K.: LCIA, 2020.

[12] M. L. Moses, *The Principles and Practice of International Commercial Arbitration*, 3rd ed. Cambridge, U.K.: Cambridge Univ. Press, 2017.

[13] European Parliament and Council of the European Union, "Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I)," *Official Journal of the European Union*, vol. L177, pp. 6–16, Jun. 17, 2008.

[14] European Parliament and Council of the European Union, "Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II)," *Official Journal of the European Union*, vol. L199, pp. 40–49, Jul. 11, 2007.

[15] European Parliament and Council of the European Union, "Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (GDPR)," *Official Journal of the European Union*, vol. L119, pp. 1–88, Apr. 27, 2016.

[16] Singapore International Arbitration Centre (SIAC), *SIAC Arbitration Rules 2025*. Singapore: SIAC, 2022.

[17] S. C. Symeonides, *Choice of Law*. Oxford, U.K.: Oxford Univ. Press, 2016.

[18] United Nations Commission on International Trade Law (UNCITRAL), *UNCITRAL Model Law on International Commercial Arbitration (1985, with amendments adopted in 2006)*. New York, NY, USA: United Nations, 2006.

[19] United Nations, *Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York Convention)*, 330 U.N.T.S. 38, 1958.

[20] *Yahoo! Inc. v. La Ligue Contre le Racisme et l'Antisemitisme*, 433 F.3d 1199 (9th Cir. 2006).

[21] *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003).

[22] Republic of Uzbekistan, *Law of the Republic of Uzbekistan "On Arbitration"*, No. ZRU-64, Oct. 16, 2006, amended. [Online]. Available: LexUZ

[23] Republic of Uzbekistan, *Law of the Republic of Uzbekistan "On Personal Data"*, No. ZRU-547, Jul. 2, 2019, amended 2023. [Online]. Available: LexUZ Personal Data Law