Cybersecurity as due process and its limits in international arbitration

Dennis Crouch*

Principia No. Especial 1–2025 pp. 49-55

Resumen: El artículo analiza la ciberseguridad como una dimensión del debido proceso en el arbitraje internacional y examina sus límites frente a amenazas digitales avanzadas, especialmente aquellas de origen estatal. A partir de casos reales y del desarrollo reciente de instrumentos de soft law, el autor sostiene que la ciberseguridad no debe tratarse solo como una cuestión técnica o administrativa, sino como un componente esencial de la equidad procesal. Propone integrar el análisis de riesgos tecnológicos en la gestión del caso arbitral mediante criterios de proporcionalidad, sensibilidad, viabilidad y costos. No obstante, advierte que el arbitraje carece de herramientas efectivas para enfrentar interferencias cibernéticas patrocinadas por Estados, lo que obliga a replantear las expectativas sobre confidencialidad y protección procesal en la era digital.

Abstract: The article examines cybersecurity as a dimension of due process in international arbitration and explores its limits in the face of advanced digital threats, particularly those originating from state-sponsored actors. Drawing on real cases and recent soft law developments, the author argues that cybersecurity should not be treated merely as a technical or administrative issue, but as a core element of procedural fairness. He proposes integrating technological risk analysis into arbitral case management through criteria such as proportionality, sensitivity, feasibility, and cost. However, the article warns that arbitration lacks effective tools to address state-sponsored cyber interference, prompting a reassessment of traditional expectations regarding confidentiality and procedural protection in the digital era.

Palabras Claves: Ciberseguridad | Arbitraje internacional | Debido proceso | Confidencialidad | Amenazas estatales

Keywords: Cybersecurity | International arbitration | Due process | Confidentiality | State-sponsored threats

* Dennis D. Crouch es profesor Judge C.A. Leedy de Derecho en la Facultad de Derecho de la Universidad de Missouri (Mizzou Law). Es reconocido por su experiencia en propiedad intelectual e inteligencia artificial. Autor prolífico, es creador del influyente blog jurídico Patently-O. Ingeniero por Princeton y abogado por la Universidad de Chicago, ha recibido múltiples premios a la docencia.

Sumario: I. Introduction, II. The State-Sponsored Threat: A New Category of Risk, III. Integrating Technology into Arbitral Case Management, IV. The Limits of Arbitral Remedies in the Face of State Actors, V. Conclusion

I. Introduction

Yarubith Escobar Bastidas's article on cybersecurity in international arbitration provides a valuable window into how arbitral practice has entered the digital era and the attendant security implications[1]. Bastidas documents the rapid digitalization of arbitral proceedings and explains that while these innovations improve efficiency, they also expose new vulnerabilities. Her treatment of emerging "soft law"—including the ICCA-NYC Bar-CPR Protocol on Cybersecurity (2022) and the ICCA-IBA Roadmap to Data Protection (2020)—demonstrates how the arbitration community has begun developing frameworks for managing digital risks[2].

In reading the article, the most compelling aspects are her illustrations of cyber threats through case examples, including the 2015 hack of the Permanent Court of Arbitration's website during *Philippines v. China* and the alleged cyber-intrusion in *Gela Mikadze v. Ras Al Khaimah Investment Authority*. These incidents underscore that cyber breaches in arbitration have already materialized with potentially serious consequences: exposure of sensitive data, procedural disruption, and challenges to award enforcement.

For arbitral tribunals, malicious cyber interference strikes at core values of due process. When hackers can infiltrate proceedings and skew outcomes, the integrity of the arbitral process itself is at risk[3]. This response adds to the discussion with the argument that technological considerations such as cybersecurity must be integrated into due process analysis[4]. In other words, it is not merely an administrative concern, but is a fundamental component of procedural fairness in the digital age. When parties entrust sensitive filings to cloud servers or hold hearings on videoconferencing platforms, they create new vectors for procedural unfairness.

But the difficulties here are immense. International hackers operate across jurisdictional boundaries where traditional legal enforcement mechanisms prove in-

[1] Yarubith Escobar Bastidas, *Ciberseguridad en el Arbitraje Internacional*, *Principia*, Edición Especial 1 (2025).

[2] ICCA–NYC Bar–CPR, *Protocol on Cybersecurity in International Arbitration* (2022 ed.); ICCA–IBA, *Roadmap to Data Protection in International Arbitration* (Consultation draft 2020).

[3] *ICCA–NYC Bar–CPR, Protocol on Cybersecurity in International Arbitration, 16–17.*

[4] Stephanie Cohen y Mark Morril, "A Call to Cyberarms: The International Arbitrator's Duty to Avoid Digital Intrusion," *Fordham International Law Journal* 40 (2017): 983–84; Klaus Peter Berger y J. Ole Jensen, "Due Process Paranoia and the Procedural Judgment Rule: A Safe Harbour for Procedural Management Decisions by International Arbitrators," *Arbitration International* 32, no. 3 (2016): 415.

effective, making accountability and remediation extraordinarily challenging. State-sponsored actors compound these problems exponentially, wielding sophisticated resources and operating with near-impunity under sovereign protection, creating threats that existing arbitral frameworks are simply not equipped to address. These realities force uncomfortable questions about arbitration's traditional promises–particularly whether meaningful confidentiality can be maintained against determined state actors, and what the arbitration community can realistically achieve in protecting proceedings from sovereign cyber operations."

II. The State-Sponsored Threat: A New Category of Risk

Unlike opportunistic cybercriminals motivated by quick profit, state-sponsored hackers conduct sophisticated, sustained operations through advanced persistent threats[5]. These adversaries are well-funded and patient, capable of deploying zero-day exploits and remaining hidden in arbitral IT systems for extended periods while gathering intelligence. Their methods and resources far outstrip those of ordinary hackers. But despite common wisdom on the extent of state-sponsored hacking, attributing these incursions to particular states is notoriously difficult[6]. State-backed groups often disguise their digital fingerprints or plant false flags to mislead investigators, obscuring who is behind a breach. This creates troubling accountability and enforcement gaps that can permit these sovereign shielded malicious actors to operate with near impunity and certainly beyond the direct reach of arbitral control.

Certain disputes are especially vulnerable to state-backed intrusion – or perhaps I should say more likely to be targeted. Cases involving defense technology, energy concessions, critical infrastructure, or emerging technologies represent potential intelligence goldmines. The current era of rising economic competition and technological rivalry between major powers creates powerful incentives for state actors to target arbitral proceedings for strategic advantage. When disputes touch on technologies or industries deemed essential to national competitiveness, the potential rewards of cyber-espionage far outweigh the risks of detection.

Although many incidents do not become public –especially those involving arbitration– there are still more than a handful of publicly shared incidents that illus-

[5] Nanda Rani, Bikash Saha y Sandeep Kumar Shukla, "A Comprehensive Survey of Advanced Persistent Threat Attribution: Taxonomy, Methods, Challenges and Open Research Problems," arXiv:2409.11415v1 (7 de septiembre de 2024), https://arxiv.org/abs/2409.11415v1; William Akoto, "State-Sponsored Cyber Attacks and Co-Movements in Stock Market Returns: Evidence from US Cybersecurity Defense Contractors," *Business and Politics* 27 (2025): 95.

[6] Delbert Tran, Note, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack," *Yale Journal of Law & Technology* 20 (2018): 376.

trate this reality. In 2014, the U.S. Department of Justice indicted five members of a Chinese military-affiliated hacking unit for infiltrating American nuclear, steel, and solar companies to steal trade secrets for state-owned enterprises[7]. The 2015 hack of the Permanent Court of Arbitration during *Philippines v. China* demonstrates that even supposedly neutral arbitral institutions are not immune when geopolitical stakes are high[8].

III. Integrating Technology into Arbitral Case Management

Arbitrators already balance efficiency, fairness, and cost in procedural decisions under established case management principles. The challenge is explicitly recognizing how technology intersects with these existing duties. Rather than creating entirely new doctrines, tribunals can adapt familiar proportionality analysis to address digital-age concerns.

Historically, cybersecurity has been treated as purely an IT issue. And, it is certainly a technical problem for system administrators and support staff. But, the emerging soft law instruments represent an important evolution, shifting cybersecurity into case management and administration, where arbitral institutions and procedural coordinators address digital risks as part of organizing proceedings. This administrative layer builds upon the IT foundation while recognizing that cybersecurity has procedural implications.

However, this approach does not go far enough. Treating cybersecurity as an administrative matter still risks separation from core legal decisions and the arbitrators who make them. Grounding cybersecurity considerations directly in due process doctrine ensures that these concerns reach the tribunal itself—the ultimate guardians of procedural fairness. And, it provides them with flexible legal grounding to exercise their inherent authority over procedural matters when digital threats emerge, rather than relegating such decisions to institutional administrators who lack both legal authority and intimate knowledge of the specific case dynamics.

The due process principles are built upon the same case management structure. One practical approach for tribunals is to analyze cybersecurity decisions along multiple dimensions: the cybersecurity risk profile of the case, the sensitivity of information involved, the technical feasibility for all parties, and the associated costs. This framework builds on existing soft law guidance while ensuring

[7] *"U.S. to Charge Chinese Workers with Cyberspying," New York Times, 20 de mayo de 2014.*
[8] *"Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims?," The Diplomat, 27 de octubre de 2015.*

that no single factor dominates the analysis[9].

Risk assessment involves evaluating the nature of the dispute, parties involved, and potential consequences of security breaches. High-stakes investment or emerging technology cases may justify stronger protective measures than routine commercial disputes.

Sensitivity analysis considers the confidentiality and privacy interests at stake. Cases involving trade secrets, personal data, or national security information warrant heightened protection, as breaches would undermine fundamental party rights.

Feasibility evaluation ensures technological solutions remain accessible to all participants. Due process includes maintaining a level playing field—sophisticated cybersecurity tools that only well-funded parties can navigate may inadvertently create unfairness[10].

Cost proportionality requires that security measures remain reasonable relative to the dispute. The ICCA-CPR Protocol explicitly advises giving "special consideration to what measures may be taken without significant expenditure," recognizing that excessive costs can deny access to justice[11].

This multi-factor approach is not prescriptive but rather provides a structured way for tribunals to exercise their existing case management discretion while addressing technological considerations systematically.

IV. The Limits of Arbitral Remedies in the Face of State Actors

Traditional arbitral remedies assume wrongdoers subject to tribunal authority. These are parties bound by the arbitration agreement and the resulting award. This framework breaks down entirely when confronting cyber threats from external actors, particularly state-sponsored hackers operating under sovereign protection. They cannot be summoned before arbitral tribunals, sanctioned for misconduct, or compelled to provide curative disclosure. The traditional arsenal of arbitral remedies—cost-shifting, evidence exclusion, procedural modifications—may address symptoms but cannot reach the source of state-sponsored interference.

This lack of meaningful after-the-fact remedies makes preventive cybersecurity measures so much more important. Yet even enhanced cybersecurity

[9] *ICCA–NYC Bar–CPR, Protocol on Cybersecurity in International Arbitration, Schedule B; ICC Commission on Arbitration and ADR, ICC Commission Report on Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings (2022).*

[10] ICC Commission Report on Leveraging Technology for Fair, Effective and Efficient International Arbitration Proceedings, 15, 32.

[11] ICCA–NYC Bar–CPR, *Protocol on Cybersecurity in International Arbitration*, Commentary to Principle 6.

measures have limits. No defensive system can guarantee protection against nation-state adversaries with unlimited resources and sophisticated capabilities.

Individual tribunals cannot solve this problem alone. Meaningful protection may require coordination among arbitral institutions, national cybersecurity agencies, and international organizations. We effectively need an international commitment that simply does not exist today – especially because each nation-state is looking to simultaneously close and exploit security breaches.

International arbitration organizations could work with cybersecurity agencies to develop sector-specific guidance for high-risk disputes. In extreme cases, coordination with diplomatic or security agencies might be necessary when arbitrations touch on matters of genuine national security concern. However, such coordination raises troubling questions about arbitral neutrality and independence. If arbitral institutions partner too closely with state security agencies, they risk appearing to serve particular national interests rather than neutral dispute resolution. The arbitration community must also recognize what it cannot achieve. Individual tribunals cannot deter all state-sponsored cyber operations driven by national security considerations. This recognition should inform realistic expectations about arbitral cybersecurity.

These cybersecurity challenges force a deeper reckoning with arbitration's traditional commitment to confidentiality. If state actors can routinely penetrate arbitral proceedings, the promise of private dispute resolution becomes increasingly illusory. This erosion raises fundamental questions about what we are fighting to preserve–how vigorously should the arbitration community defend what amounts to a system of secret courts?

The benefits of arbitral confidentiality are real: protecting trade secrets, encouraging settlement, and facilitating candid evidence presentation. But these advantages come at a price of public accountability and now rising technical security costs. If confidentiality cannot be reliably maintained against determined state actors, should arbitration's value proposition shift away from privacy and toward other advantages such as efficiency, expertise, and enforceability? Cybersecurity threats make these questions unavoidable.

V. Conclusion

Due process in international arbitration must evolve to address digital-age challenges while maintaining core fairness principles. This does not require revolutionary changes to arbitral doctrine, but rather explicit recognition that technological choices carry due process implications.

The arbitration community should treat technology decisions with the same care

given to other procedural matters. At case commencement, tribunals and parties should discuss technological arrangements—covering e-disclosure protocols, hearing formats, cybersecurity measures, and data privacy requirements—with transparency and reasoned decision-making.

The goal is not technological perfection but proportionate responses to identified risks. As arbitration continues to digitalize, the community must ensure that procedural fairness keeps pace with technological innovation. By integrating cybersecurity and technology considerations into established due process frameworks, arbitration can maintain its promise as a fair and effective dispute resolution mechanism while embracing digital transformation.