

INFUSION OF TECHNOLOGY AND CYBERSECURITY IN INTERNATIONAL ARBITRATION



SAHAJA BURDE

The Author is a third year student pursuing BA. LL.B (Hons.) at ILS Law College, Pune

Introduction

Although Alternative Dispute Resolution (“ADR”) is considered preferential over adversarial litigation due to its fundamental nature of collaborative solution-finding, cost and time effectiveness, its popularity amongst parties increased as a dispute resolution mechanism because of its distinct features – confidentiality and privacy. Rapid technology strides have evolved ADR into a much more effective, efficient, and convenient mechanism. But coupled with this, is the increase in cybersecurity risks, rendering the distinct features of the mechanism questionable.

The practical application of Information Technology (“IT”) in International Arbitration ranges from electronic communications, storage of information in fixed or portable storage media to hearing room technologies.[1] The information involved in international arbitrations is highly vulnerable considering that the parties are often multi-national companies or non-governmental organizations. Such parties are already potential targets for cybersecurity attacks. In the event of parties being governments or public entities, the publicity of such cases is high, putting the information shared at an increased risk.[2] This article aims to analyze the cybersecurity risk involved in international arbitrations and the institutional responses to the same.

Cybersecurity Risk Quotient

There exist two main factors for the increase in cyber threats. The first is, the gradual increase in the digitalization of arbitral practice. While legal practitioners worked even before technological strides, hacking grew with the onset of digitalization. Lawyers and arbitrators worked with papers and voluminous documentation before the infusion of technology. Hence, adapting to the change is a gradual process for them, which is not the case for hackers and data thieves.

Secondly, there exists no express prohibition with regard to the acceptance of illegally obtained information as evidence in arbitration proceedings.[3] In an arbitration, the admissibility of evidence is at the discretion of the arbitral tribunal and the 'IBA Rules on the Taking of Evidence in International Arbitration' ("IBA Rules") is widely accepted while considering the same.[4]

Article 9 of the IBA Rules provides for exclusion of evidence on the ground of 'failure of party to conduct itself in good faith in the taking of evidence',[5] thereby excluding information obtained illegally by parties directly from the domain of admissible evidence. But the admissibility of illegally obtained information by a third party to the arbitration still remains a grey area. After the case of WikiLeaks,[6] multiple incidences of parties using leaked information as evidence were recorded. In *Conoco Phillips v. Venezuela*,[7] the Respondent approached the tribunal seeking a reconsideration of the tribunal's decision on the grounds of new evidence. The evidence mentioned were communications between concerned diplomats which was obtained via WikiLeaks. The tribunal set aside the respondent's plea on the ground that it had no power to reconsider its decision but did not address the question on the admissibility of the evidence. However, the dissenting opinion relied on the new information implying the acceptance of such hacked information as evidence.

Subsequently, in *Caratube v. Kazakhstan*,[8] the question of admissibility was addressed. The tribunal accepted the evidence obtained via WikiLeaks and iterated that any information available in the public domain would be accepted as evidence. Considering the above, a party in an arbitration proceeding may obtain information by illegal means and ask any third party to publish it, making it available to the public and hence, qualifying it as evidence.[9]

An additional factor to the rise in cyber threats is the differing levels of cybersecurity mechanisms in an arbitration. Each participant in an arbitration - law firms, solo practitioners, parties to the case, and arbitrators, would respond to the posing cyber threat in varying degrees. While law firms might have a well-devised cybersecurity system, it may be challenging for solo practitioners and parties to cope with the threat.[10] It, thus, becomes a shared responsibility and an error by which one can cause irrevocable damage to all.

Towards Mitigation of Risk– Institutional Responses

In July 2015, on the third day of hearing of a maritime border dispute between China and the Philippines in the Permanent Court of Arbitration (“PCA”), Hague, the Court’s website was hacked, allegedly by Chinese cyber units. A malicious code was placed on the website and the computers of every diplomat, lawyer, or any other who visited the website were infected.[11] In the wake of such an event, cybersecurity risk in arbitration and especially in international arbitration has seen greater emphasis and combating responses. A malicious code was placed on the website and the computers of every diplomat, lawyer, or any other who visited the website were infected.[11] In the wake of such an event, cybersecurity risk in arbitration and especially in international arbitration has seen greater emphasis in combating responses.

The International Council for Commercial Arbitration (“ICCA”) in association with the New York City Bar Association (“NYCBA”) and the International Institute of Conflict Prevention & Resolution (“CPR”) launched a Working Group on Cybersecurity in International Arbitration. The Working Group has come up with a ‘Protocol on Cybersecurity in International Arbitration (2020 Edition)’.[12] The protocol is drafted to “provide a framework to determine reasonable information security measures for individual arbitration. It is intended to create awareness about information security in international arbitrations”. Although the protocol does not impose any liability, it effectively raises awareness and is expected to evolve further in light of changing technology, new cyber threats and regulations. Additionally, the International Bar Association (“IBA”), recognizing the cyber threat to law firms, has prescribed the ‘Cyber Security Guidelines (2018)’.[13] The document promotes efficient utilization of technology and working with IT professionals. Considering that most cyberattacks are a result of human error, the importance of educating personnel is deeply emphasized under the broad categories of ‘organizational processes’ and ‘staff training’. The International Chamber of Commerce (“ICC”) has prepared the ‘ICC Cyber Security Guide’[14] for businesses. It comprises key principles of cybersecurity, essential security actions, tips for development of cybersecurity policies and a self-assessment questionnaire. Both these guides lay down practical defense mechanisms that may be incorporated by firms, companies, and enterprises to mitigate the risk of cyber breaches.

The International Centre for Dispute Resolution (“ICDR”) has implemented ‘Secure Case Administration’^[15] with best practice policies, technologies, and procedures to deter data thefts.

Concluding Remarks

A development in understanding the gravity of cybersecurity in international arbitration has been notable. But the data threats are reasonably anticipated to not just increase but become more complex and sophisticated. Arbitral institutions will be required to revise their combat regime occasionally and accordingly. The active participation of every member in an arbitration is necessary in addition to institutional responses. Parties in an arbitration must be encouraged to agree on cybersecurity protocols that establish sufficient safeguards. Arbitrators must train and equip themselves to secure all information provided to them. Law firms must inculcate best practices to safeguard all valuable information that they might possess. Such action is not just essential to protect the interests of parties in an arbitration and avoid damage or loss but also to safeguard the dispute resolution mechanism itself.

ENDNOTES-

- [1] INFORMATION TECHNOLOGY IN INTERNATIONAL ARBITRATION, ICC, (2017), <https://iccwbo.org/content/uploads/sites/3/2017/03/icc-information-technology-in-international-arbitration-icc-arbitration-adr-commission.pdf>.
- [2] Anca M Sattler, *Cybersecurity threats in arbitration are real: Why take a risk?*, ADR INST. OF CAN. (Feb. 22, 2018) <http://adric.ca/adr-perspectives/cybersecurity-threats-in-arbitration-are-real-why-take-a-risk/>.
- [3] Shook Hardy and Bacon, *Managing Cyber and Data Risk in Arbitration*, CORP. DISP. MAG., (June 2019), <https://www.shb.com/-/media/files/professionals/a/anglesgiovanni/angles-cd-mrqa.pdf>.
- [4] *Evidence – ICSID Convention Arbitration*, INT'L CTR. FOR SETTLEMENT OF INV. DISP. (hereinafter "ICSID"), <https://icsid.worldbank.org/en/Pages/process/Evidence-ICSIDConventionArbitration.aspx>.
- [5] IBA RULES ON THE TAKING OF EVIDENCE IN INTERNATIONAL ARBITRATION, INT'L B. ASS'N, (May 2010), https://www.ibanet.org/ENews_Archive/IBA_30June_2010_Enews_Taking_of_Evidence_new_rules.aspx.
- [6] Martand Jha, *What was WikiLeaks All About? : A Classic Case of Cyber Security*, INDIAN DEF. REV., (Sept. 6, 2017), <http://www.indiandefencereview.com/spotlights/what-was-wikileaks-all-about-a-classic-case-of-cyber-security/>.
- [7] ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v. Bolivarian Republic of Venezuela. ICSID Case No. Arb/07/30, (Mar. 10, 2014).
- [8] Caratube International Oil Company LLP and Devincei Salah Hourani v. Republic of Kazakhstan. ICSID Case No. Arb/13/13, (Sep. 27, 2017).
- [9] *Admissibility of Hacked Emails as Evidence in Arbitration*, N.Y.U. TRANSNAT'L NOTES, (May 14, 2018), https://blogs.law.nyu.edu/transnational/2018/05/admissibility-of-hacked-emails-as-evidence-in-arbitration/#_ftn21.
- [10] Steven A. Certilman & Eric W. Wiechmann, *ADR in the Age of Cybersecurity*, 12 NYSBA N.Y. DISP. RESOL. LAW., (2019), <https://nysba.org/NYSBA/Publications/Section%20Publications/Dispute%20Resolution/Article-DisputeResolutionLawyer%20Spring2019.pdf>.
- [11] Jason Healey and Anni Piiparinen, *Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims?*, THE DIPLOMAT, (Oct. 27, 2015), <https://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/>.
- [12] Protocol on Cybersecurity in International Arbitration, International Council for Commercial Arbitration, (2020), https://www.arbitration-icca.org/media/14/76788479244143/icca-nyc_bar-cpr_cybersecurity_protocol_for_international_arbitration_-_print_version.pdf.
- [13] CYBER SECURITY GUIDELINES, INT'L B. ASS'N, (Oct. 2018), <https://www.ibanet.org/LPRU/cybersecurity-guidelines.aspx>.
- [14] ICC CYBER SECURITY GUIDE FOR BUSINESS, ICC, (2015), <https://iccwbo.org/content/uploads/sites/3/2015/08/ICC-Cyber-Security-Guide-for-Business.pdf>.
- [15] *Secure Case Administration*, INT'L CTR. FOR DISP. RESOL. https://www.icdr.org/Secure_Case_Administration.