ISSN : 1875-4120
Issue : Vol. 16, Issue 3
Published : May 2019

This paper is part of the TDM Special Issue on **"Cybersecurity in International Arbitration"** prepared by:

Stephanie Cohen
Independent Arbitrator
View profile

Mark C. Morril
MorrilADR
View profile

Transnational Dispute Management
www.transnational-dispute-management.com

Cyber Intrusion as the Guerrilla Tactic: An Appraisal of Historical Challenges in an Age of Technology and Big Data by E. Sussman

About TDM

TDM (Transnational Dispute Management): Focusing on recent developments in the area of Investment arbitration and Dispute Management, regulation, treaties, judicial and arbitral cases, voluntary guidelines, tax and contracting.

Visit www.transnational-dispute-management.com for full Terms & Conditions and subscription rates.

Open to all to read and to contribute

TDM has become the hub of a global professional and academic network. Therefore we invite all those with an interest in Investment arbitration and Dispute Management to contribute. We are looking mainly for short comments on recent developments of broad interest. We would like where possible for such comments to be backed-up by provision of in-depth notes and articles (which we will be published in our 'knowledge bank') and primary legal and regulatory materials.

If you would like to participate in this global network please contact us at info@transnational-dispute-management.com: we are ready to publish relevant and quality contributions with name, photo, and brief biographical description - but we will also accept anonymous ones where there is a good reason. We do not expect contributors to produce long academic articles (though we publish a select number of academic studies either as an advance version or an TDM-focused republication), but rather concise comments from the author's professional 'workshop'.

TDM is linked to **OGEMID**, the principal internet information & discussion forum in the area of oil, gas, energy, mining, infrastructure and investment disputes founded by Professor Thomas Wälde.

Cyber Intrusion as the Guerrilla Tactic: An Appraisal of Historical Challenges in an Age of Technology and Big Data*

by Edna Sussman[1]

"There is a new mantra in cybersecurity today, *"it's when not if."*[2]

Introduction

Cyber intrusion and hacking are in the news almost daily with damaging invasions of law firms, corporations, governmental agencies, and political entities. "Security breaches are becoming so prevalent that there is a new mantra in cybersecurity today: 'It's when not if,' a law firm or other entity will suffer a breach."[3] Those who monitor IT systems report dozens of attempted attacks on a daily basis. Arbitration participants have not been immune.

This article seeks to flag for further analysis: (a) arbitrators duties with respect to cybersecurity risks, (b) admissibility of illegally obtained documents, (c) authentication of documents, (d) sanctions, (e) the psychological impact on decision-making of inadmissible evidence, and (f) the arbitrator's duty to report.

The Arbitrators' Duties

At the ICCA Conference in 2018, a consultation draft of the Cybersecurity Protocol For International Arbitration was circulated for comment. The Protocol is "intended to encourage participants in international arbitration to become more aware of cybersecurity risks in arbitration and to provide guidance that will facilitate collaboration in individual matters about the cybersecurity measures that should reasonably be taken, in light of those risks and the individualized circumstances of the case to protect information exchange and the arbitral process."[4] It is hoped that adherence to the Protocols coupled with adherence to practical guidance on how to protect against cyber intrusion will diminish the number of incidents in international arbitration.

Guidance on how arbitrators should manage their practice in light of today's cyber risk have been emerging and arbitrators would be well advised to consult those sources and consider whether they should undertake some cyber security measures in their practice.[5] Users of

---

* The full version of this article will be published in Jean Kalicki and Mohamed Abdel Raouf, eds., *Evolution and Adaptation: The Future of International Arbitration*, ICCA Congress Series no. 20 (Kluwer, forthcoming).

[1] Edna Sussman esussman@sussmanadr.com is an independent arbitrator and a member of the panel of many of the leading dispute resolution institutions around the world. She serves as the distinguished ADR Practitioner in Residence at Fordham Law School and serves on the Board of the American Arbitration Association, as the chair of the AAA-ICDR Foundation, as Vice-Chair of the New York International Arbitration Center and is a past President of the College of Commercial Arbitrators.

[2] David Reis, *ABA Tech Report 2017*, A.B.A., https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html (last visited May 23, 2018).

[3] *Id.*

[4] *Draft Cybersecurity Protocol for International Arbitration – Consultation Draft*, ICCA-NYC Bar-CPR, http://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf at p.5 (last visited May 23, 2018).

[5] *See*, *e.g.*, Stephanie Cohen & Mark Morril, *A Call to Cyber Arms: the International Arbitrators Duty to Avoid Digital Intrusion*, 40 FORDHAM INT'L. L. J., 981 (2017); Jill D. RHODES & ROBERT S. LITT, THE ABA

arbitration are entitled to expect that arbitrators will take at least basic security measures and it is anticipated that user expectations in this regard will increase in the coming years. Steps taken now can avoid problems in the future. Many measures can be taken that are neither expensive nor difficult. This is a subject that no arbitrator can safely ignore.

Admissibility

Arbitrators have broad discretion in dealing with evidence under applicable laws and institutional rules. Given this wide discretion and the binding nature of arbitral awards, tribunals generally admit evidence to avoid risking vacatur for failure to provide a full and fair opportunity to present the case, and then consider its credibility, weight and value. However, on a proper showing evidence may be excluded by the arbitral tribunal.

Where it is demonstrated that evidence has been obtained illegally the arbitral tribunal is faced with a difficult choice. With the prevalence of cyber intrusions in today's world, it is inevitable that tribunals will be increasingly required to address the question of whether or not they should admit illegally obtained evidence. However, no clear line of authority has developed to guide tribunals as to how they should treat illegally obtained evidence. Tribunals have arrived at different conclusions on the question.[6]

Illegally obtained evidence is not new, but it is likely to be more prevalent in this age of technology and big data. The classic case dealing with illegally obtained evidence is the 2005 decision in *Methanex v. United States* (*Methanex*), long before WikiLeaks, in which the tribunal declined to admit the evidence.[7] Methanex attempted to rely on documents obtained by going through wastepaper and rubbish in support of its position. The tribunal stressed the general duty of good faith and the fundamental principles of justice and fairness and declined to admit the evidence, although it also considered the question of materiality of the evidence and concluded that it was only of "marginal evidential significance."[8]

In the well-known Yukos award which granted $50 billion in damages, the tribunal relied extensively on confidential diplomatic cables from the United States Department of State that had been illegally obtained and published on WikiLeaks.[9] The tribunal provided no analysis of whether evidence illegally obtained should be admitted. Other published awards in investor state cases have specifically addressed the admissibility of evidence illegally obtained through cyber intrusion. *See e.g., Libananco v. Turkey* (counsel communications

---

CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (2d ed. 2018); ARBITRATION IN THE DIGITAL AGE: THE BRAVE NEW WORLD OF ARBITRATION (Maud Piers & Christian Aschauer eds., 2018); ARIAS•U.S, PRACTICAL GUIDE FOR INFORMATION SECURITY IN ARBITRATION (2017).

[6] For a discussion of the arbitral decisions addressing the admissibility of evidence obtained through cyber intrusion. *See,* Cherie Blair & Ema Vidak Gojković, *WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence*, 22(1) ICSID Rev. – For. Inv. L. J. 1 (2018); J. H. Boykin & M. Havalic, *Fruits of the Poisonous Tree: The Admissibility of Unlawfully Obtained Evidence in International Arbitration,* 5 TRANSNAT'L DISP. MGMT. J. (2015); Jessica O. Ireton, *The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of Wikileaks Cables as Evidence*, 30(1) ICSID REV. – FOR. INV. L. J. 231 (2015).

[7] NAFTA Chapter Eleven Arbitral Tribunal: Methanex Corporation v. United States of America, Final Award on Jurisdiction and Merits - August 3, 2005 - Text of Decision, 44 I.L.M. 1345 (2005).

[8] *Id.*, at ¶ 56.

[9] Hulley Enters. Ltd. (Cyprus) v. Russian Fed'n, PCA Case No. AA 226, Final Award, 1185–86 (Jul. 18, 2014) [hereinafter Hulley]. The District Court of The Hague quashed the final award from Hulley on other grounds on April 20, 2016. As of this writing the appeal is pending.

intercepted-not admitted); *Caratube v. Kazakhstan* (hackers uploaded government documents-11 introduced, those not privileged admitted), *Conoco Phillips v. Venezuela* (after an interim decision material documents were made public on WikiLeaks-court declined to reconsider its decision and did not consider the evidence; strong dissent).

The decisions appear to emphasize who committed the wrongful act, whether the documents are privileged, and whether the information revealed was material to the decision on the merits. Balancing the search for truth and other values is not new. It is just being presented in a new context in our digital world. As William Park said, "Nothing new resides in balancing truth-seeking against values that further public goals rather than adjudicatory precision."[10]

Authentication

Litigation positions taken by parties with the ascendance of cyber intrusion may be presented in a variety of ways. A party may contend that the documents were "stolen" by hacking into his or her IT system; thus, illegally obtained. That contention raises questions of admissibility discussed above. A party may contend that it no longer has the documents available for production because it was hacked. That contention raises questions of proof as with any assertion that documents no longer exist. Or illegally hacked emails might be posted publicly on WikiLeaks or some other platform on the web that is publicly available. Again, that raises a question of admissibility discussed above. The party may contend that the emails were fabricated by a hacker and that they did not write it. That contention raises questions of authenticity.

Authentication is not an issue frequently encountered in international arbitration. However, it is likely that with the prevalence of cyber intrusions and the ease with which it seems to be possible to intrude, arbitrators will likely be required to review an increasing number of objections to admissibility based on lack of authenticity.

Sanctions

The question of what sanctions a tribunal has authority to impose, and when and how sanctions should be imposed has been the subject of extensive discussion in recent years in the wake of the issuance of the 2013 International Bar Association Guidelines on Party Representation in International Arbitration (IBA Guidelines). Various proposals have been made as to who should be responsible for sanctioning counsel. Cyber intrusion brings that issue to the fore.

Tribunals are appropriately concerned about guerrilla tactics, and consideration of remedies beyond the exclusion of evidence may be appropriate in cases of cyber intrusion. As the tribunal stated in *Libananco*:[11] "The Tribunal attributes great importance to privilege and confidentiality, and if instructions have been given with the benefit of improperly obtained privileged or confidential information, severe prejudice may result. If that event arises the

[10] William W. Park, *Truth Seeking in International Arbitration*, in THE SEARCH FOR "TRUTH" IN ARBITRATION: IS FINDING THE TRUTH WHAT DISPUTE RESOLUTION IS ABOUT? 1, 10 (Markus Wirth et al. eds., 2011). For a comprehensive decision which directly addresses the balance between the competing policy imperatives of truth and privilege in the context of WikiLeaks exposure, *See, Wee Shuo Woon v. HT S.R.L.,* [2017] S.G.C.A. 23 (Sing.)

[11] Libananco Holdings Co. Ltd. v. Republic of Turkey, ICSID Case No. ARB/06/8, Decision on Preliminary Issues at ¶ 80 (Jun. 23, 2008).

Tribunal may consider other remedies available apart from the exclusion of improperly obtained evidence or information."

The IBA Guidelines empower the tribunal to address "misconduct" by a party representative after giving the parties notice and a reasonable opportunity to be heard. Misconduct is broadly defined by the IBA Guidelines to include "breach of the present guidelines, or any other conduct that the arbitral tribunal determines to be contrary to the duties of a party representative." The nature of the "misconduct" intended to be covered has not been established but, certainly, cyber intrusion would fall into that category. In determining the remedy, the tribunal is to consider the nature and gravity of the misconduct, the good faith of the party representative, the extent to which the party representative knows about or participated in the misconduct, the potential impact of a ruling on the rights of the parties, the need to preserve the integrity and fairness of the arbitral proceedings, and the enforceability of the award. These considerations clearly outline the matters to be considered in deciding whether or not to impose a sanction on a party for cyber intrusions, if it is concluded that the tribunal has authority to do so.

The Impact on Decision-Making of Inadmissible Evidence

Study after study has established that fact finders cannot ignore inadmissible information and are influenced in their decision-making by that information, even if it has been excluded. As Doron Teichman and Eyal Zamir sum up the literature: "[n]umerous studies have documented the effects of inadmissible evidence in … legal domains, such as hearsay evidence, pretrial media reports, and illegally obtained evidence. These studies show that inadmissible evidence affects judicial decision-making in civil as well as criminal settings, irrespective of whether that evidence favors the prosecution or the defense. A recent meta-analysis concluded that 'inadmissible evidence produced a significant impact.'" [12]

As the courts have found it can be "difficult to 'unring the bell.'"[13]Arbitrators should be sensitive to this unconscious influence and carefully assess the evidence upon which they rely to ensure that it supports their conclusions without reference to excluded evidence. Advocates should be sensitive to the fact that highlighting evidence to urge its exclusion may cause it to make an even deeper impression on the fact finder.

Duty to Report

Cyber intrusion is a crime in jurisdictions around the world. Violations of privacy laws is also implicated. What, if any, is the arbitrator's duty to report a cybercrime? And to whom? Local authorities? Counsel's bar association? The administering institution? While arbitrators must first consider whether they are under any legal or ethical obligation that requires them to take action, the resolution of the question presents the tension between reporting wrongdoing and the confidentiality of the arbitration proceeding.

Elliott Geisinger and Pierre Ducret distinguish between doctored documents and witnesses lying on the stand, which they consider sufficiently dealt with by the tribunal's disregard of

[12] Doron Teichman et al., *Judicial Decision-Making: A Behavioral Perspective*, *in* OXFORD HANDBOOK OF BEHAVIORAL ECONOMICS AND THE LAW 1, 9 (Eyal Zamir et al. eds., 2014). *See also*, Andrew J. Wistrich et al., *Can Judges Ignore Inadmissible Information? The Difficulty of Deliberately Disregarding*, 153 U. PA. L. REV. 1251, 1279–81 (2005).
[13] N.L.R.B. v. Jackson Hosp. Corp., 257 F.R.D. 302, 307 (D.D.C. 2009).

such evidence on the one hand and what they referred to as a "Balrog"[14] on the other hand. A Balrog is a violation of fundamental national or supranational rules close to transnational public policy. They cite as examples, money laundering, corrupt practices, gross violation of competition law, fraudulent conveyances, financing of terrorism, violation of embargoes, traffic of cultural property, and gross violations of environmental regulations.[15] If a party hacks into another parties' computer system, or worse yet, posts it publicly or provides it to others to post publicly, one might well conclude that the matter involves no ordinary doctored document, but rather rises to the level of a Balrog.

However, Geisinger and Ducret conclude that finding a reporting duty is in complete contradiction with the confidential nature of international commercial arbitration and suggest that most legal systems would not impose any such duty even with respect to Balrogs. They allow for possible exceptions for extremely serious violations of fundamental legal principles such as human trafficking where the confidentiality of the arbitration becomes a "minor consideration."

The question of when an arbitrator has a duty report is likely to be a continuing discussion not only in the context of cyber intrusions but also in connection with other unlawful acts.

Conclusion

The ease with which it appears cyber intrusion can be accomplished and the almost daily reports of hacks suggests that arbitrators are likely to increasingly be presented with issues related to breaches of cyber security. The issues are not new. They are merely presented in a new guise. It is hoped that this article will lead to further analysis of the issues raised in this context.

[14] The Balrog reference draws upon Tolkien's Lord of the Rings tale of miner dwarves who dug too deeply and unleashed "a terrible daemon from ancient times," the Balrog.

[15] Elliott Geisinger & Pierre Ducret, *The Uncomfortable Truth: Once Discovered What to do With it*, in THE SEARCH FOR "TRUTH" IN ARBITRATION: IS FINDING THE TRUTH WHAT DISPUTE RESOLUTION IS ABOUT? 113, 114 (Markus Wirth et al. eds., 2011).