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

By Edna Sussman

“There is a new mantra in cybersecurity today, “it’s when not if.””

INTRODUCTION

Cyber intrusion and hacking is 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.” Those who monitor IT systems report dozens of attempted attacks on a daily basis. Arbitration participants have not been immune.

At the ICCA conference in 2018, a consultation draft of Protocols for Cyber Security in International Arbitration was circulated for comment. The Protocols are “designed to be adopted in individual international arbitration matters on a case-by-case basis following a risk analysis of relevant circumstances” in order to determine reasonable cyber security measures. 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.

---


2 Id.

3 See e.g., Allison Ross, Cybersecurity and Confidentiality Shocks for the PCA, Global Arbitration Review (July 23, 2015) (reporting on a hack of the PCA website during the hearing of the maritime border dispute between the Philippines and China.); Zachary Zagger, Hackers Target Anti-Doping, Appeals Bodies Amid Olympics, Law360.com (Aug. 12, 2016) (hackers attempted to infiltrate the website of the Court of Arbitration for Sport during the Rio Olympic Games).

4 Add citation when available

5 Following are some of the currently available sources that address cybersecurity measures but technology is constantly evolving and hackers are increasingly sophisticated and developing new cyber weapons. Keeping up to date on the latest guidance is essential. See e.g., Stephanie Cohen
While guerrilla tactics such as fabricated or illegally obtained evidence are not new, cyber intrusion requires a review of pertinent issues that might arise where fabricated or illegally obtained evidence is made possible by virtue of cyber intrusion. This article seeks to flag for further analysis (a) the issues that may arise and that may require consideration by arbitrators in instances in which evidence is introduced at the hearing which is, or is claimed to be, hacked or fabricated through cyber manipulation; (b) unconscious influences that can impact decisions where such evidence is an issue; and (c) the arbitrator’s duties when confronted with such evidence. The discussion will provide an overview of the admissibility of illegally obtained documents, authentication of documents, sanctions, the psychological impact on decision-making of inadmissible evidence, the influence of one’s native legal culture on decision-making and the arbitrator’s duty to report.

**Admissibility of illegally obtained evidence**

Arbitrators have broad discretion in dealing with evidence. They may admit or reject evidence, and have full discretion in evaluating and weighing the evidence in determining what weight, if any, the evidence should be given. Article 19 (2) of the UNCITRAL Model Law provides that “[t]he power conferred upon the arbitral tribunal includes the power to determine the admissibility, relevance, materiality and weight of any evidence.” National laws governing the arbitration provide similar powers to the arbitrators.\(^6\)

The IBA rules and institutional rules grant broad discretion to the arbitral tribunal in the taking of evidence. Article 9(1) of the 2010 the IBA Rules on the Taking of Evidence provides that “[t]he arbitral tribunal shall determine the admissibility, relevance, materiality and weight of evidence.” Article 20(6) of the 2014 ICDR rules provides that “[t]he tribunal shall determine the admissibility, relevance, materiality and weight of the evidence.” Rule 34 (a) of the 2013 AAA Rules provides that “[C]onformity to legal rules of evidence shall not be necessary.” Rule

22.1(vi) of the 2014 LCIA rules provide that the tribunal “shall have the power …to decide whether or not to apply any strict rules of evidence (or any other rules) as to the admissibility, relevance or weight of any material tendered by a party on any issue of fact…”

The courts recognize the discretion afforded to arbitrators and consistent with the deference courts generally give arbitral decisions, courts have confirmed that arbitral tribunals are not bound by domestic rules of evidence. “In practice, international arbitral tribunals typically do not apply strict rules of evidence, particularly rules of evidence applicable in domestic litigations.”

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. Reporting on a dispute before a federal court in New York an aptly named article in the Wall Street Journal was titled Hackers for Hire are Easy to Find. Hundreds of a Kuwaiti billionaire’s personal emails were posted online available to all. It was reported that the cost for the hackers was $400 demonstrating the low cost and ease with which computer hacking can be accomplished.

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.

---

7 See e.g. Bell Aerospace v. Local 516, 500 F.2d 921, 923 (2d Cir.1974 ) (“in handling evidence and arbitrator need not follow all the niceties observed by the federal courts”)

8 Born, supra n.6 at 2310.

9 Edna Sussman, The Arbitrator Survey – Practices, Preferences and Changes on the Horizon, Amer. Rev. Int’l. Arb., Vol. 26, No. 4 at 521 ( 2015) (survey results demonstrated that only 11% of arbitrators excluded evidence that would not be admissible under national evidentiary standards more than 75% of the time).


The Corfu Channel case, heard before the International Court of Justice between 1947 in 1949 was an early instance in which the tribunal dealt with illegally obtained evidence. The United Kingdom in violation of Albania’s sovereignty conducted a mine sweeping operation in Albania waters to find evidence in support of its case that Albania had failed to give warning to the United Kingdom about mines in the channel as was required by international law, which caused several British warships to be struck by submerged mines. While the court found that the United Kingdom’s actions were unlawful, the court did not exclude the evidence and did not apply any material sanctions against the United Kingdom.

Taking a different position in the prominent arbitration decision in Methanex Corporation v. United States of America, long before WikiLeaks, the tribunal declined to admit the wrongfully obtained evidence. Methanex attempted to rely on documents obtained through 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:

[I]t would be wrong to allow Methanex to introduce this documentation into these proceedings in violation of its general duty of good faith and, moreover, that Methanex’s conduct, committed during these arbitration proceedings, offended basic principles of justice and fairness required of all parties in every international arbitration.”

The Methanex tribunal however, also considered the question of materiality of the evidence and concluded that it was only of “marginal evidential significance.”

In the well-known Yukos award the tribunal, which awarded $50 billion in damages, relied extensively on confidential diplomatic cables from the United States Department of State that had been illegally obtained and published on WikiLeaks. The tribunal specifically referenced the views expressed by officials in the U.S. Embassy’s cables published by WikiLeaks in support of its decision stating that the cables revealed the “candid” and “unguarded” views of PwC’s


12 Corfu Channel Case (UK v Albania) (Merits) [1949] ICJ Rep 4.


14 Id. Para. 59.

15 Id. Para. 56.

16 Hully Enterprises, Limited v Russian Federation, Award paras. 1185 – 86 (July 18, 2014) . The Hague District Court quashed the award on other grounds on April 20, 2016.
senior management, an important issue in the case. The tribunal provided no analysis of whether evidence illegally obtained should be admitted.

In *Libananco v. Turkey,* while the arbitration was in progress, Turkish authorities were intercepting Libananco’s electronic communications, including between Libananco and its legal counsel, and obtained 2,000 legally privileged and confidential emails. Turkey maintained that the surveillance activities had nothing to do with the arbitration and the files intercepted were not shared with the department that was handling the arbitration. The tribunal referenced as having been affected: basic procedural fairness, respect for confidentiality and legal privilege, the right of parties to advance their respective cases freely and without interference and respect for the tribunal itself. The tribunal expressed the principle that “[p]arties have an obligation to arbitrate fairly and in good faith and that an arbitral tribunal has the inherent jurisdiction to ensure that this obligation is complied with.” The tribunal directed that any document which had been intercepted which related to the arbitration be destroyed and held that any privileged documents or information which may be introduced in the future as well as any evidence derived from possession of such documents or information would be excluded from evidence.

In *Caratube v. Kazakhstan* Caratube attempted to introduce 11 documents that had been made publicly available on the Internet as a consequence of a hacking of Kazakhstan’s government IT system. Hackers had uploaded about 60,000 documents onto a website known as “Kazakhleaks.” The tribunal allowed the admission of all non-privileged leaked documents but excluded from the record all illegally leaked privileged documents finding that the tribunal must "afford privileged documents the utmost protection."
The application for reconsideration of an interim decision in Conoco Phillips v. Venezuela provides an example of the potential for flash points between the search for truth and other values. \[23\] Venezuela, in an application for reconsideration of an interim decision relied on U.S. Embassy cables made available on WikiLeaks which showed that Venezuela had attempted to negotiate in good faith with the claimant, including about compensation for the expropriation and which directly contradicted previous factual findings of the tribunal. The challenge was rejected based on the tribunal’s analysis of the right to reconsider a prior decision under the ICSID rules, concluding that its prior decision had res judicata effect and could not be reconsidered. In a strong dissent Professor George Abi-Saab, concluding that the revelations of the WikiLeaks cables, which he found to be reliable, radically contradicted the factual analysis of the prior decision, stated:

“In the circumstances, I don’t think that any self-respecting Tribunal that takes seriously its overriding legal and moral task of seeking the truth and dispensing justice according to the law on that basis, can pass over such evidence, close its blinkers and proceed to build on its now severely contestable findings, ignoring the existence and the relevance of such glaring evidence.”

It would be shutting itself off by an epistemic closure into a subjective make-believe world of its creation; a virtual reality in order to fend off probable objective reality; a legal comedy of errors on the theatre of the absurd, not to say travesty of justice, that makes mockery not only of ICSID arbitration, but of the very idea of adjudication.”\[24\]

That the discretion afforded to arbitrators calls upon them to balance the search for truth and other values is not new. It is just being presented in a new context in our digital world. As Park said, “nothing new resides in balancing truth-seeking against values that further public goals rather than adjudicatory precision.”\[25\] As Park elaborated:

Arbitrators are supposed to arrive at some understanding of what actually happened and what legal norms determine the parties’ claims and defenses. In finding facts and applying law, arbitrators should aim at getting as near as reasonably possible to a correct view of


\[24\] Id. Dissent on Respondent's Request for Reconsideration at 24.

the events giving rise to the controversy, and to consider legal norms applied in other disputes that raise similar questions.

This does not mean that arbitrators do not balance truth-seeking against other goals. Indeed, they do so all the time, notably in connection with document production (which competes with economy in speed), and attorney-client privilege (which inhibits attempts to get at what corporate officers really knew). However, since balancing the interests does not require abandonment of truth taking as an aspiration.\(^\text{26}\)

In short, there are no bright lines that govern the admissibility of illegally obtained evidence, as is the case with many of the instances with the tribunal is called upon to balance competing values. 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.

Blair and Gojkovic, in their comprehensive article analyzing the existing jurisprudence conclude that a trend may be discerned based on existing case law. They posit that the “legal and policy elements which have been taken into account when deciding admissibility of illegally obtained evidence include:

(i) Has the evidence been obtained unlawfully by a party who seeks to benefit from it?

(ii) Does the public interest favour rejecting the evidence as inadmissible?

(iii) Do the interests of justice favor the admission of evidence.”\(^\text{27}\)

As decisions continue to explicate the question of admissibility of evidence that is the fruit of a cyber intrusion, other issues and concerns present themselves that bear analysis.

**Authentication**

While this discussion focuses on emails, similar issues can arise with texts, Facebook entries and postings on other social media outlets. Litigation positions taken by parties with the ascendance of cyber intrusion are presented in a variety of ways. A party may contend that the documents were “stolen” by hacking into his or her IT system and thus illegally obtained.\(^\text{28}\) That contention


\(^{27}\) Blair and Gojkovic, *supra*, n. 11 at 25. *See also*, Boyken and Havalic *supra* n. 11 (distilling the decisions to provide a roadmap for analysis of admissibility).

\(^{28}\) See discussion of the *Kazakhstan* case above.
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, although a forensic examination may be required for the production of such proof in the context of digital evidence. 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 they did not write it. That contention raises questions of authenticity discussed in this section.

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.

In a famous case the plaintiff alleged that while he was at Harvard Facebook’s CEO, Mr. Zuckerberg, entered into a “work-for-hire” contract pursuant to which plaintiff helped fund the development of Facebook in exchange for a one half interest in Facebook. The authenticity of the purported contract and of several related emails were challenged. Given the magnitude of what was at stake a variety of forensic examination tools were employed, including a review of the metadata, backdating anomalies, formatting anomalies, and a linguistic analysis. Each of these forensic tests is discussed by the court at length in its decision. Based on its conclusion that the purported contract and the emails were not authentic but a recently created fabrications, the court relying on its inherent authority concluded that the case could not go to the jury and dismissed.

For arbitrators faced with determining authenticity, a review of factors which may be considered under the U.S. Federal Rules of Evidence may be instructive in determining authenticity. In addition to evidence as to digital hash values and testimony from a forensic witness as to when the email issued and from which device based on the metadata and other features, Graham,


30 See, e.g., Republic of Kazakhstan v. Ketebaev, 2017 WL 6539897 (N.D. Ca. 2017), (describing a hacking of emails of Kazakh government employees, which were posted on a website and posted on personal Facebook pages and newspaper websites and included attorney-client communications between Kazakh officials and their attorneys; the case was dismissed for lack of personal jurisdiction).

Capra and Joseph identify a variety of circumstantial factors that may be considered and could be useful to arbitrators confronted with this issue. 32

They conclude that “[w]hile it is true that an email may be sent by anyone who, with a password, gained access to another’s email account, similar questions could be raised with traditional documents… The mere fact that hacking, etc., is possible is not enough to exclude an email or any other form of digital evidence…. If the mere possibility of electronic alteration were enough to exclude the evidence, then no digital evidence could ever be authenticated.” 33

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 IBA Guidelines on Party Representatives in International Arbitration (“IBA Guidelines”). 34 Various proposals have been made as to who should be responsible for sanctioning counsel. 35 Guerrilla tactics, including cyber intrusion, bring 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: “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 Tribunal may consider other remedies available apart from the exclusion of improperly obtained evidence or


33 Id. at 9.


35 See, e.g. Elliott Geisinger, Soft Law and Hard Questions: ASA’s Initiative in the Debate on Counsel Ethics in International Arbitration, in THE SENSE AND THE NON-SENSE OF GUIDELINES, RULES AND PARA-REGULATORY TEXTS IN INTERNATIONAL ARBITRATION, ASA Special series no. 37 (2015) (proposing a global arbitration ethics council); Tom Jones and Alison Ross, Mourre Calls for Institutions to Join Forces, Global Arbitration Review (March 9, 2018) (noting that “ASA’s proposal did not attract international consensus because important institutions …took the view that counsel misconduct is for arbitrators to deal with support from institutions.”)
information.”

Sanctions that have been considered as potentially appropriate include negative inferences, cost sanctions, disqualification of counsel, and even in particularly egregious cases, a dismissal of the entire case with prejudice.

While drawing negative inferences does not raise serious questions about the authority of the tribunal, the question of whether the tribunal has the power to impose cost sanctions on the parties and even more questionably on counsel has not been firmly settled. Mayer “opined that punishing a counsel or party through a decision on costs is an abuse of the power to sanction. This is because an arbitrator is not allowed to impose a penalty without a basis in law: “[W]ithout a power specifically conferred either by the law or by the parties ... an arbitrator is not allowed to impose a penalty.” Others have suggested that the power to impose cost sanctions should be more vigorously pursued, as arbitration users have urged. Authority might be found in institutional rules, party adoption of the IBA Guidelines, party agreement and perhaps even the tribunal’s inherent power. Some courts have confirmed the tribunal’s authority to impose costs as a sanction.

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 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 within that category. The guidelines give the tribunal power to respond and specifically identify admonishing the party representative, drawing inferences, apportioning

36 Libananco supra n. 18 at para. 80.
37 Born, supra n. 6 §15.10.
40 White & Case, Queen Mary University of London School of International Arbitration, 2012 International Arbitrations Survey: Current and Preferred Practices in the Arbitral Process, 41 (reporting that according to the survey, an overwhelming majority of respondents believe tribunals should take into account improper conduct by a party or its counsel when allocating costs).
41 See cases cited in Born, supra n. 6 at 2316 – 2317.
costs, and taking other “appropriate measures in order to preserve the fairness and integrity of the proceeding.” 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 know 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 state the matters to be considered in deciding whether or not to impose costs on a party for cyber intrusions if it is concluded that the tribunal has authority to do so.

Whether or not the tribunal has the authority to disqualify counsel in international arbitration has also not been definitively decided. The historical view has been that arbitral tribunals do not have the power to disqualify or sanction counsel. However, that may be evolving. In the leading case, *Hrvatska Elektroprivreda, d.d. v Republic of Slovenia*, the tribunal disqualified counsel brought into the representation shortly before the hearing which presented a conflict with one of the arbitrators based on the inherent power of the tribunal to take measures to “preserve the integrity of the proceedings.” In a subsequent case the tribunal in *Rompetrol Group N.V. v. Romania* declined to disqualify counsel, and while, not deciding the limits of the tribunal’s powers, stated that “such powers as may exist would be one to be exercised only rarely, and in compelling circumstances.”

Given the right of the parties in arbitration to select a representative of their choosing, any power to disqualify counsel will certainly be very sparingly

---


43 Catherine Rogers, *ETHICS IN INTERNATIONAL ARBITRATION*, at 135 (Oxford University Press Publ. 2014).

44 *Hrvatska Elektroprivreda, d.d. v Republic of Slovenia*, Tribunal’s ruling regarding the participation of David Mildon QC in further stages of the proceeding ICSID ARB/05/24 (May 6, 2008).

45 *The Rompetrol Group N.V. v. Romania*, decision of the Tribunal on the participation of a counsel, ICSID Case No. ARB/06/3 (January 14, 2010).
exercised. Courts, however, in appropriate circumstances, have not hesitated to disqualify counsel who have engaged in a cyber guerrilla tactic.

The dismissal of the entire case with prejudice as a sanction for guerrilla tactics would be an extreme measure and not likely to be the remedy chosen by a tribunal. Horvath and Wilske report that no tribunal has done so. Courts have not always been so restrained and have dismissed complaints lodged by parties who have engaged in illegal conduct in the collection of evidence by cyber intrusion.

The impact on decision-making of inadmissible evidence

National laws provide exclusionary evidentiary rules where the prejudicial effect of the evidence outweighs its probative value, where the nature of the evidence has limited reliability and therefore limited probative value or where policy considerations dictate exclusion as is the case in disincentivizing illegal behavior. While these exclusionary evidentiary rules authorize and in some cases require the fact finder to exclude the evidence, the fact is that the fact finder has already seen the 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 Teichman and 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

46 Alan Scott Rau, Arbitrators Without Powers? Disqualifying Counsel in Arbitral Proceedings, Arbitration International Vol. 30 Issue 3, 457-512, at 511 (2014) (“Precisely because of their regulatory spareness, transnational rules will have the virtue of directing the attention of arbitral tribunals to the core of what alone is critical – – that is, to what is minimally necessary to ensure the fairness of proceedings.”)

47 See e.g. ____________________________

48 GUERRILLA TACTICS supra n. 39 at 51-52; Gunther J. Horvath, Stephan Wilske and Jeffrey C Leng, Lessons to be Learned for International Arbitration GUERRILLA TACTICS supra n.39 at 278-289.

49 See e.g., Leor Exploration & Production, LLC. v. Aguiar, 2010 WL 3782195 (S.D. Florida 2010)(dismissing the case in which the party had engaged in computer hacking relying on the court's inherent power to impose sanctions for bad-faith conduct and finding that no lesser sanction would suffice under the circumstances); Salmeron v. Enterprise Recovery Systems, 579 F.3d 787 (7th Cir. 2009) (dismissing the case as a sanction for the willful leak of documents which were ultimately posted on WikiLeaks).
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.’”

Illustrative study outcomes include one study which demonstrated that there was a spread in finding liability as between judges who saw inadmissible privileged information damaging to the plaintiff (29% found for plaintiff) as compared to judges who did not see that information (55% found for the plaintiff). There was a spread of 25% in the damages awarded between judges who saw evidence of an unrelated criminal conviction which was suppressed as unduly prejudicial and those who were not informed of the prior criminal conviction. Recognition of unconscious influence is undoubtedly the rationale for not permitting parties to introduce evidence of settlement discussions.

As the courts have found it can be “difficult to ‘unring the bell.’” 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.

**The impact on decision-making of native legal culture**

At a recent conference, a well-known arbitrator suggested that looking to the law of one’s own jurisdiction is very useful in considering whether the governing law makes sense. Those in attendance were surprised by that comment, but it was perhaps just a conscious recognition of the fact that at an unconscious level one’s own legal culture, whether native or the one in which an individual has predominantly practiced, may influence one’s analysis and decision.

Supporting this conclusion Joshua Karton found in his study of the evolution of contract law in arbitration, that tribunals considered extrinsic evidence where they were charged with applying the law of a common law jurisdiction even though the law of that jurisdiction would have

---


precluded such evidence.\textsuperscript{53} We can surmise that this outcome resulted from the influence of the arbitrators’ native legal culture. As Guiditta Cordero-Moss aptly put it “the legal background of the arbitrator is recognized as playing an important role, a sort of imprinting, which will influence the approach taken…”\textsuperscript{54} Thus, while the award may be written with reference to the applicable law, the conclusion may be driven by an arbitrator’s legal culture. As Justice Scalia pointed out, quoting Chancellor James Kent who said, “I most always found [legal] principles suited to my views of the case.”\textsuperscript{55} National laws may vary as to the admissibility of unlawfully obtained evidence and influence decisions on admissibility of evidence obtained through cyber intrusion.\textsuperscript{56}

A comprehensive decision reviewing prior relevant authorities was issued by the Singapore Court of Appeals in 2016, which directly addressed the question of the balance between the competing policy imperatives of truth and privilege in the context of WikiLeaks exposure.\textsuperscript{57} A former employee sought to introduce into evidence communications of his former employer with its counsel, which had been hacked by unknown parties and uploaded onto WikiLeaks. The court concluded that even though the WikiLeaks material submitted as evidence was publicly available, because it constituted a minute fraction of the approximately 500 GB of data that had been pilfered just from the former employees’s system, it was highly probable that few, if any, knew of its existence, and therefore the contents were not public knowledge and retain their confidential status. The court considered the fact that the employee had not been the perpetrator of the cyber attack but concluded there was little doubt that the employee knew that the emails were privileged. The court held that the confidential character the information in the emails had not been lost by its posting on WikiLeaks because to hold otherwise would be to “sanction and to encourage unauthorized access and pilferage of confidential information.” The court further examined whether or not the documents supported the conclusions the employees sought to draw


\textsuperscript{56} See, Jane Colston, \textit{The Fruit from a Poisoned Tree-Use of Unlawfully Obtained Evidence}, IBA International Litigation Newsletter 20-24 (September 2017).

from them and concluded that they did not. The court concluded that “the balance between the competing imperatives of truth and privilege is … struck in favor of the latter.”

Historically the United Kingdom case law supported accepting evidence which had been obtained in violation of law or ethics. In 1980 an English court opined that in civil cases “the judge cannot refuse it [evidence] on the ground that it may have been unlawfully obtained in the beginning.” That statement of principle may be in the process of evolving and considerations of competing values are being reviewed in light of subsequent enactments. In a decision issued in 2003, the court considered violations of the Human Rights Act committed by an insurer which filmed a video of the claimant in her home without her knowledge, having obtained access to the claimant’s home by deception. The court weighed the circumstances against the relevance of the evidence and concluded “this is not a case where the conduct of the defendant’s insurers is so outrageous that the defence should be struck out… It would be artificial and undesirable for the actual evidence, which is relevant and admissible, not to be placed before the judge who has the task of trying the case.”

But in an even more recent case in 2010 documents had secretly been accessed and copied for the wife from the husband’s server in his office and passed on to the wife’s solicitor. The court narrowed the Hildebrand rules which was previously thought to permit access to information about the other spouse whether or not it was confidential to assist in proceedings concerning financial provision. The court held that where rights pursuant to Article 8 of the Human Rights Act and expectations of privacy are breached return of documents was required. The court noted that the conduct in question might also have constituted criminal offenses under the Computer Misuse Act 1990 and the Data Protection Act 1998. In rendering its decision, the court stated that it had given due regard to the competing rights to a fair trial, to confidence and to rely on evidence.

---

58 Id. at 29.


61 Cooper supra n. 59.

62 Jones v University of Warwick [2003] EWCA Civ 151.

In the United States, in order to safeguard Fourth Amendment rights, the exclusionary rule does not permit the admission of evidence seized during an unlawful search as proof at a criminal trial. The courts have developed the “fruit of the poisonous tree” doctrine which extends the exclusionary rule to require suppression of other evidence that is derived from and is tainted by the illegal search or seizure. The doctrine is not applicable in civil cases. How courts handle evidence derived through illegal or unethical means in civil cases is not uniform and is generally fact specific. Courts have said that “[g]enerally in civil cases, the manner in which evidence is obtained is irrelevant to the issue of admissibility.” On the other hand, the courts have noted that “courts routinely preclude use of evidence obtained in violation of the ethical rules in order to appropriately remedy that violation.”

Addressing an application to strike references to documents that had been released by others on WikiLeaks from the complaint, a U.S. court declined to do so. The court found that since the “documents have been available in the public domain for more than five years,… [The] court does not have the power or ability to limit its access…. The court cannot effectively enforce an injunction against the Internet and its various manifestations, and it would constitute a dubious manifestation of public policy were to attempt to do so.” The complaint “does not put this material ‘in the public eye’ any more than the Internet has already done so”.

Taking a contrary and negative view of the issue, it has been reported that in France the use of documents known to be illegally obtained would be a criminal offence and regarded as contrary to international public policy.

---

64 Lingo v. City of Salem, 832 F.3d 953 (9th Cir. 2016); White v City of Birmingham, 96. F. Supp. 3d 1260, 1271 ( N.D. Ala. 2015) (noting that the Supreme Court has “repeatedly declined to extend the exclusionary rule to proceedings other than criminal trials” and permitting the evidence, noting its immense probative value.)


68 Alison Ross, Tribunal Rules on Admissibility of Hacked Kazakh Emails, Global Arbitration Review (September 22, 2015) (reporting on counsel’s reliance on this French law and efforts to persuade the exclusion of the hacked emails); Accord, Colston supra n. 55 ( citing Assemble pleniere, Cour de Cassation, 7 January 2011, No. 09-15.316 0914.667)
In light of the unconscious influence of one’s native legal culture there may be situations where counsel would wish to consider emphasizing differences, if there are any, between the applicable law and the native legal culture of the arbitrators.

**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? 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.

Geisinger and Ducret distinguish between doctored documents and witnesses lying on the stand which they consider sufficiently dealt with by the tribunal’s disregard of such evidence on the one hand and what they referred to as a “Balrog” 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. If a party hacks into another party’s 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 and rises to the level of a Balrog.

---


71 The Balrog reference draws upon Tolkien’s Lord of the Rings tale of miners-dwarves who dug too deeply and unleashed “a terrible deamon from ancient times,” the 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.”

Two anecdotes confirm the general acceptance of Geisinger and Ducret’s conclusion. It became clear to the tribunal in the course of one hearing, when the testimony of one witness was interrupted by counsel and both counsel requested an adjournment that the testimony revealed a Balrog which had not previously been identified. The tribunal approached the arbitral institution and requested a formal legal opinion as to their duties. A British QC was retained to deliver an opinion virtually overnight. He opined that the tribunal did not have a duty to report the Balrog. The tribunal relied on that advice. In another case, it became apparent from the testimony that a bridge was in imminent danger of collapse because the steel that had been used in its construction was not of sufficient thickness. The tribunal advised counsel that if they did not report it to the authorities promptly the tribunal would take it upon itself to do so.

Perhaps the bright line between reporting a Balrog and preserving confidentiality is drawn when there is a danger to life and limb.

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 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 assist arbitration practitioners in understanding the issues as presented in this context and provide guidance as to how to approach them.

Edna Sussman esussman@SussmanADR.com is a full time independent arbitrator and is the Distinguished ADR Practitioner in Residence at Fordham University School of Law. She was formerly a litigation partner at White & Case LLP and has served in as an arbitrator in over 200 complex commercial arbitrations, both international and domestic, under many institutional rules and ad hoc. Ms. Sussman is a member of the panel of many of the leading dispute resolution institutions around the world and is a fellow of the Chartered Institute of Arbitrators. She sits on the Board of the American Arbitration Association, serves as the chair of the AAA-ICDR Foundation, is Vice-Chair of the New York International Arbitration Center

73 Id. see authorities cited at 128-130; See also, Mourre supra n. 70.
and is a past President of the College of Commercial Arbitrators. A graduate of Barnard College and Columbia Law School, Ms. Sussman has lectured and published widely on arbitration, mediation, energy and environmental issues.