Cyber Espionage in Inter-State Litigation

Marco Benatar[*]

I. Introduction: The Dangers of the Digital Domain

Growing anxiety over cyber security is fuelling efforts to put the use of information and communications technologies (ICTs) on a firmer legal footing. This sentiment is aptly expressed by the Secretary-General of the United Nations (UN):

> Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.[1]

As global and regional organizations direct their energies toward the international regulation of ICTs, so too do individual States, many of which have integrated international law in their cyber doctrines. The allure of cyberspace has also captivated researchers, who have produced a prodigious body of literature on topics as varied as *jus ad bellum* and human rights.[2] Within this broader scholarly conversation, cyber espionage is rapidly becoming a core concern.[3] The keen interest undoubtedly stems from the

---

* Research Fellow at the Max Planck Institute Luxembourg for Procedural Law.

1 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174, 22 July 2015, para. 4 [GGE Report 2015].

2 See M. Benatar, Cyber Warfare, in A. Carty (ed.), Oxford Bibliographies in International Law (2014), available at: http://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0087.xml?rskey=YzkK10&result=1&q=Cyber+Warfare#firstMatch (last visited 23 October 2018).

3 See e.g. D. Weissbrodt, Cyber-Conflict, Cyber-Crime, and Cyber-Espionage, 22 Minnesota Journal of International Law (2013), 347; C. S. Yoo, Cyber Espionage or Cyberwar? International Law, Domestic Law, and Self-Protective Measures, in J. D. Ohlin et al. (eds.), Cyberwar: Law and Ethics for Virtual Conflicts (2015), 175; R. Buchan, The International Legal Regulation of State-Sponsored Cyber Espionage,

barrage of revelations that continue to surface in the media. Detailed accounts of mass electronic surveillance programs,[4] the interception of communications of Heads-of-State[5] and the theft of industrial secrets[6] regularly make world headlines.

Clandestine ICT activities have even spread to inter-State litigation,[7] as came to light in the recent *South China Sea Arbitration*. This closely-fol-

---

in A.-M. Osula and H. Rõigas (eds.), International Cyber Norms: Legal, Policy & Industry Perspectives (NATO Cooperative Cyber Defence Centre of Excellence, 2016), 65; K. Ziolkowski, Peacetime Cyber Espionage – New Tendencies in Public International Law, in K. Ziolkowski (ed.), Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (NATO Cooperative Cyber Defence Centre of Excellence, 2013), 425; D. Pun, Rethinking Espionage in the Modern Era, 18 Chicago Journal of International Law (2017), 353.

4 A. Deeks, An International Legal Framework for Surveillance, 55 Virginia Journal of International Law (2015), 291; I. Georgieva, The Right to Privacy under Fire: Foreign Surveillance under the NSA and the GCHQ and its Compatibility with Art. 17 ICCPR and Art. 8 ECHR, 31 Utrecht Journal of International and European Law (2015), 104; P. Margulies, The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism, 82 Fordham Law Review (2014), 2137; M. Milanovic, Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age, 56 Harvard International Law Journal (2015), 81; D. Yernault, De la fiction à la réalité: le programme d'espionnage électronique global 'Echelon' et la responsabilité internationale des Etats au regard de la Convention européenne des droits de l'homme, 33 Revue belge de droit international (2000), 137; J. J. Paust, Can You Hear Me Now?: Private Communication, National Security, and the Human Rights Disconnect, 15 Chicago Journal of International Law (2015), 612.

5 S. Talmon, Das Abhören der Kanzlerhandys und das Völkerrecht, 1 Bonner Rechtsjournal (2014), 6.

6 D. P. Fidler, 'Economic Cyber Espionage and International Law: Controversies involving Government Acquisition of Trade Secrets through Cyber Technologies' (2013), available at: https://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving (last visited 23 October 2018); C. Lotrionte, Countering State-Sponsored Cyber Economic Espionage under International Law, 40 North Carolina Journal of International Law and Commercial Regulation (2015), 443; C. Parajon Skinner, An International Law Response to Economic Cyber Espionage, 46 Connecticut Law Review (2014), 1165.

7 As the focus of this paper is inter-State litigation, cases involving national security before human rights bodies will not be covered. See e.g. ECtHR Research Division, 'National Security and European Case-Law' (2013), available at https://rm.coe.int/168067d214 (last visited 23 October 2018). In international commercial arbitration (another area not treated in this chapter), the threat posed by malicious cyber actors has prompted soft law initiatives. See Draft Cybersecurity Protocol for International Arbitration, 2018, available at https://www.arbitration-icca.org/media/10/43322709923070/draft_cybersecurity_protocol_final_10_april.pdf (last visited 23

lowed case, administered by the Permanent Court of Arbitration (PCA), saw the Philippines challenge China's maritime claims and activities in the South China Sea.[8] In 2015, on the third day of hearings in the Peace Palace (The Hague), a cyber-attack originating from China took down the PCA's website for an extended period, leaving the page infected with malware luring unsuspecting online visitors.[9] Compounding matters further, forensic investigations led an IT security company to conclude that an actor based in China had targeted the computer systems of groups involved in the maritime spat. The hit list included the law firm representing the Philippines in the arbitration and the malicious program used in the attack is known to enable data exfiltration from the victim's compromised machine.[10]

Should this be a harbinger of things to come, international courts and tribunals could soon face credible allegations that parties appearing before them have spied on each other using cyber capabilities. A likely scenario is one whereby a party to the proceedings retrieves information from the adverse party or its representatives to get a leg up in the ongoing litigation.

To be sure, in many instances the allegations will remain just that, given the arduous task of substantiating covert intelligence gathering and its attribution to the opposing State.[11] Past cases show the difficulty of proving acts of espionage to the tribunal's satisfaction. Following the 1979 storm-

---

October 2018); Debevoise Protocol to Promote Cybersecurity in International Arbitration (2017), available at https://www.debevoise.com/~/media/files/capabilities/cybersecurity/protocol_cybersecurity_intl_arb_july2017.pdf (last visited 23 October 2018); L. Yong, Working Group Unveils Cybersecurity Protocol at ICCA (2018), available at https://globalarbitrationreview.com/article/1168043/working-group-unveils-cybersecurity-protocol-at-icca (last visited 23 October 2018); C. Morel de Westgaver, Cybersecurity in International Arbitration – A Necessity and an Opportunity for Arbitral Institutions (2017), available at http://arbitrationblog.kluwerarbitration.com/2017/10/06/cyber-security/ (last visited 23 October 2018).

8 South China Sea Arbitration (Philippines v. China), Award of 12 July 2016, PCA Case No. 2013-19.

9 J. Healey and A. Piiparinen, 'Did China Just Hack the International Court Adjudicating Its South China Sea Territorial Claims?' (2015), available at http://thediplomat.com/2015/10/did-china-just-hack-the-international-court-adjudicating-its-south-china-sea-territorial-claims/ (last visited 23 October 2018). Shortly after the incident, the International Court of Justice issued an announcement on its website notifying visitors that it was a distinct institution from the PCA and had no involvement in the aforementioned case.

10 F-Secure, 'NanHaiShu: RATing the South China Sea' (2016), available at https://www.f-secure.com/documents/996508/1030745/nanhaishu_whitepaper.pdf (last visited 23 October 2018).

11 Espionage on the part of counsel is not covered in this contribution. On the treatment of misconduct in international proceedings from the perspective of profes-

ing of the United States Embassy in Teheran and taking of American diplomatic and consular staff as hostages, the US took its dispute with Iran to the International Court of Justice (ICJ). Although the respondent State boycotted the proceedings, Iranian authorities made numerous statements accusing the US of conducting espionage on its soil. Noting that the assertions were unsupported by evidence, the Court dismissed Teheran's claims.[12] Closer to the present day is the ill-fated arbitration between Croatia and Slovenia which was rocked by revelations that Slovenia's agent and party-appointed arbitrator had engaged in unlawful *ex parte* communications.[13] In proceedings addressing the consequences of the incident, Slovenia floated the possibility of Croatia being behind the wiretapping of the damning telephone conversation. Lacking hard proof, the Arbitral Tribunal did not discuss the matter further.[14]

The use of ICTs adds a thick layer of complexity owing to the anonymous architecture of cyberspace and the abundant methods for wiping

---

sional ethics, see generally A. Sarvarian, Professional Ethics at the International Bar (2013); C. Parajon Skinner, Ethical Dilemmas in Inter-State Disputes, 68 Alabama Law Review (2016), 281. See also T. W. Wälde, "Equality of Arms" in Investment Arbitration: Procedural Challenges, in K. Yannaca-Small (ed.), Arbitration Under International Investment Agreements: A Guide to the Key Issues (2010), 161, 161-162 (acknowledging the existence of spying by private parties in relation to investment arbitration). Equally beyond the remit of this study is spying against the tribunal itself. Breaches of the confidentiality of deliberations are taken seriously. The Nuclear Tests case between Australia and France is illustrative of this point. Shortly before the reading of an order indicating provisional measures, statements were made and the Australian press had reported on the expected outcome of the request for provisional measures and how the judges would vote. The ICJ adopted a resolution criticizing the disclosure and launched an investigation to identify the source of the leak, which was not discovered. Nuclear Tests (Australia v. France), Judgment, Declaration of President Lachs, ICJ Reports 1974, 253, 273; Ibid., Joint Declaration of Judges Bengzon, Onyeama, Dillard, Jiménez de Aréchaga and Sir Humphrey Waldock, 273; B. Fassbender, Article 54, in A. Zimmermann et al. (eds.), The Statute of the International Court of Justice: A Commentary, 2nd ed. (2012), 1355, 1359.

12 United States Diplomatic and Consular Staff in Tehran (United States of America v. Iran), Judgment, ICJ Reports 1980, para. 82.

13 Ill-fated, but not without a silver lining, see T. Meshel, The Croatia v. Slovenia Arbitration: The Silver Lining, 16 The Law and Practice of International Courts and Tribunals (2017), 288.

14 Arbitration Between the Republic of Croatia and the Republic of Slovenia (Croatia v. Slovenia), Partial Award of 30 June 2016, PCA Case No. 2012-04, para. 211. See also A. Sarvarian and R. Baker, 'Arbitration between Croatia and Slovenia: Leaks, Wiretaps, Scandal (Part 3)' (2015), available at https://www.ejiltalk.org/arbitration-between-croatia-and-slovenia-final-part-3/ (last visited 23 October 2018).

tracks.[15] Pinning conduct to a specific State can therefore present a greater challenge than in the case of 'traditional' espionage. Attribution is harder still where non-State proxies are called on to do the spying, as their conduct will only be attributed to the State if it exerts a certain threshold of control over them.[16]

But what if, for argument's sake, the international tribunal were to conclusively determine that cyber espionage connected to the pending case has occurred and can be attributed to one of the parties? This is the question that lies at the heart of the present chapter as it seeks to address two main challenges the tribunal could realistically face. The first is whether the adjudicator can find the spying State in breach of international law and, if so, on what grounds. The second challenge is how the tribunal should treat evidence that has been procured through clandestine ICT activities.

II. General International Law and its Gaps

Let us assume that a party has established that it was the victim of cyber espionage at the hands of the opposing party and that the spying has a nexus with the ongoing proceedings. The next step is for the tribunal to formulate an appropriate response. This section will survey the range of considerations that could factor into the adjudicator's thought process. It will be demonstrated that despite the ethical misgivings one might have about spying, commentators generally hold that international law does not ban such behaviour outright. *A fortiori*, the lawfulness of ICT covert operations is at the very least uncertain. In a subsequent part, the impact of the underlying litigation will be studied. The inquiry will therefore shift to rules and principles of international dispute settlement that could be invoked to reach a finding of illicit conduct.

---

15 K. Kittichaisaree, Public International Law of Cyberspace (2017), 32-36.

16 See C. Antonopoulos, State Responsibility in Cyberspace, in N. Tsagourias and R. Buchan (eds.), Research Handbook on International Law and Cyberspace (2015), 55; P. Margulies, Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility, 14 Melbourne Journal of International Law (2014), 1; S. J. Shackelford and R. B. Andres, State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem, 42 Georgetown Journal of International Law (2011), 971.

The debate over whether the covert collection of information in peacetime,[17] i.e. absent the consent of the State controlling the information, is banned by international law has a long pedigree.[18] A few broad observations can be deduced from the voluminous literature reflecting the majority position among scholars. Most writers believe that general international law does not prohibit spying as such because none of the core norms appear to outlaw the practice.[19] Take, for instance, the principle of non-intervention. The principle is a foundational one forming part of customary international law as held by the ICJ[20] and expressed in landmark resolutions of the UN General Assembly (UNGA).[21] Non-intervention prohibits States from committing acts which are coercive and "[bear] on matters in which each State is permitted, by the principle of State sovereignty, to decide freely".[22] While actions not involving the use of force can certainly fall within the scope of non-intervention,[23] it would be difficult to argue that typical clandestine intelligence gathering meets the coercion criterion.[24]

17 This chapter does not address the law of armed conflict.

18 S. Chesterman, Secret Intelligence, in R. Wolfrum (ed.), Max Planck Encyclopedia of Public International Law (2009), para. 1, available at http://opil.ouplaw.com/home/EPIL (last visited 23 October 2018).

19 This stands in contrast to the vast number of domestic legal systems criminalizing such behaviour.

20 Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits, Judgment, ICJ Reports 1986, 14, para. 202.

21 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, GA Res. 2625 (XXV) of 24 October 1970, Annex; Manila Declaration on the Peaceful Settlement of International Disputes, GA Res. 37/10 of 15 November 1982, Annex; Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, GA Res. 36/103 of 9 December 1981, Annex; Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty, GA Res. 2131 (XX) of 21 December 1965; Draft Declaration on Rights and Duties of States, GA Res. 375 (IV) of 6 December 1949, Annex.

22 Military and Paramilitary Activities, supra note 20, para. 205.

That said, the absence of an outright prohibition does not imply that, true to the *Lotus* principle,[25] States are at liberty to spy in all circumstances without fear of breaching international law. Firstly, the international community does regulate secret intelligence albeit in a piecemeal fashion.[26] Different branches of international law place limits on espionage in circumscribed situations. A pertinent example can be found in the Vienna Convention on Diplomatic Relations (VCDR) which curtails intelligence gathering by diplomats in the receiving State.[27] Another illustration is the United Nations Convention on the Law of the Sea's (UNCLOS) exclusion of "any act aimed at collecting information to the prejudice of the defence or security of the coastal State" from the meaning of innocent passage in the territorial sea.[28]

Secondly, legal lacunae and the ubiquity of secret intelligence have not deterred States from denouncing the practice when it occurs. What matters, however, is that they do so *indirectly*: rather than claim that an act of espionage is illegal, States invoke rules which were transgressed in the process of obtaining intelligence. This roundabout approach stifles the forma-

---

23 For an assessment of various acts not involving the use of force and their compatibility with the non-intervention principle, see M. Jamnejad and M. Wood, The Principle of Non-Intervention, 22 Leiden Journal of International Law (2009), 345, 367-377. On intervention and cyberspace, see P. Wrange, Intervention in National and Private Cyberspace and International Law, in J. Ebbesson et al. (eds.), International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi (2014), 307; T. Gill, Non-Intervention in the Cyber Context, in Ziolkowski, supra note 3, 217; S. Watts, Low-Intensity Cyber Operations and the Principle of Non-Intervention, in Ohlin, supra note 3, 249.

24 Ziolkowski, supra note 3, 433. Contra Buchan, Cyber Espionage and International Law, in Tsagourias and Buchan, supra note 16, 183.

25 S.S. "Lotus" (France v. Turkey), Judgment, 1927, PCIJ Series A, No. 10, 18. See however Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, Declaration of Judge Simma, ICJ Reports 2010, 478 (calling into question the continued relevance of the Lotus principle in contemporary international law); A. Hertogen, Letting Lotus Bloom, 26 European Journal of International Law (2015), 901 (agreeing with critiques of the Lotus principle, whilst challenging the mainstream reading of the Lotus judgment).

26 Chesterman, supra note 18, paras. 23-24.

27 E.g. Vienna Convention on Diplomatic Relations, 18 April 1961, Articles 3 (1) (d), 41 (1) and (3), 500 UNTS 95 [VCDR].

28 United Nations Convention on the Law of the Sea, 10 December 1982, Art. 19 (2) (c), 1833 UNTS 397 [UNCLOS]. As for the exclusive economic zone, see E. Papastavridis, Intelligence Gathering in the Exclusive Economic Zone, 93 International Law Studies (2017), 446.

tion of a would-be *opinio juris* that renders espionage in and of itself illicit.[29] It is best exemplified by considering the response to the discovery of agents operating on foreign soil. The victim State will oftentimes treat the act as a breach of international law not because espionage is proscribed but because its territorial sovereignty has been violated.[30] A useful parallel can be drawn with the ICJ's approach in the *Military and Paramilitary Activities* case. Nicaragua had complained of US aircraft flying over its territory with the aim of intelligence gathering among other objectives. The Court did not address the lawfulness of reconnaissance in relation to the unauthorized overflights but did qualify the aerial activities as violations of Nicaraguan sovereignty under customary international law.[31]

We now turn to cyberspace which, it should be emphasized, is not a lawless domain.[32] The work of the UN Group of Governmental Experts (GGE),[33] the views of UN Member States submitted to the UN Secretary-General,[34] national cyber policies[35] and multilateral initiatives[36] all attest to the growing consensus that international law applies to computer networks. The 2015 GGE Report is noteworthy for the statement that:

29 I. Navarrete, L'espionnage en temps de paix en droit international public, 53 Canadian Yearbook of International Law (2015), 1, 7.

30 F. Lafouasse, "Le silence est d'or": réflexions juridiques sur l'espionnage entre États, in S. Cassella and L. Delabie (eds.), Faut-il prendre le droit international au sérieux? Journée d'études en l'honneur de Pierre Michel Eisemann (2016), 165, 167. See also D. Fleck, Individual and State Responsibility for Intelligence Gathering, 28 Michigan Journal of International Law (2007), 687, 692-693.

31 Military and Paramilitary Activities, supra note 20, paras. 21, 91, 251-252. Navarrete, supra note 29, 16. See also Convention on International Civil Aviation, 7 December 1944, Articles 1 and 2, 15 UNTS 295, codifying the customary rule that a State's sovereignty extends to the airspace above its land territory and territorial sea.

32 A. Pellet, Préface, in Société française pour le droit international (ed.), Colloque de Rouen: Internet et le droit international (2014), 1, 3.

33 Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98, 24 June 2013, paras. 16-25; GGE Report 2015, supra note 1, paras. 24-29. On the GGEs, see C. Henderson, The United Nations and the Regulation of Cyber-Security, in Tsagourias and Buchan, supra note 16, 465, 473-481.

> In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms.[37]

The above remarks on espionage and international law are equally valid for covert operations using cyber capabilities. The *Tallinn Manual on the International Law Applicable to Cyber Operations*, prepared by an international group of experts under the aegis of the North Atlantic Treaty Organization, corroborates this view. Rule 32 of the latest edition of the *Tallinn Manual* stipulates: "Although peacetime cyber espionage by States does not *per se* violate international law, the method by which it is carried out might do so."[38]

With this clarification in mind, the stage is set for an inquiry as to whether cyber espionage in international litigation can run afoul of international law. Assuredly, scenarios can be imagined where binding rules are violated. In those cases, an international tribunal eager to sanction the spying party could latch on to those infractions. The more intriguing question is whether breaches are *necessarily* committed. This is not a forgone conclusion: vital practical distinctions set traditional and cyber espionage apart. As mentioned earlier, the unapproved entry of secret agents in the territory of a third State is an encroachment on sovereignty. Conversely, the virtual world of interconnected servers allows for data extraction without ever set-

---

34 See UN Office of Disarmament Affairs, 'Developments in the Field of Information and Telecommunications in the Context of International Security', available at https://www.un.org/disarmament/topics/informationsecurity/ (last visited 23 October 2018).

35 E.g. United States, 'International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World' (2011), available at https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (last visited 23 October 2018).

36 E.g. International Code of Conduct for Information Security, UN Doc A/69/723, Annex, 9 January 2015 (jointly submitted by China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan).

37 GGE Report 2015, supra note 1, para. 28 (b).

38 M. N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare, 2nd ed. (2017), 168.

ting foot in the territory of the targeted State.[39] One of the surest juridical shields against espionage is thus pierced.[40] In certain respects, the situation is reminiscent of spying from outer space via satellite which several commentators do not consider to be illegal.[41] Each instance must be considered on its individual merits. By way of illustration, if the intrusion were to impair the functionality of the cyber infrastructure in the targeted State, a strong case can be built that its sovereignty has been impinged upon.[42] In sum, cyber espionage will at times fall through the gaps of general international law.

III. The Law of International Dispute Settlement as Adjudicatory Strategy

Confronted with the reality that a party has conducted cyber espionage against the opposing side, the international tribunal hearing their dispute finds itself in an unenviable position. On the one hand, there is an understandable desire to treat the act of spying as more than unethical yet lawful behaviour. On the other hand, a finding of breach might be out of step with the prevailing attitudes of States on the status of espionage, especially of the cyber kind. The dearth of relevant case law could also discourage international tribunals from taking a first bold step in tackling this contentious topic head-on. Perhaps there is an alternative to side-stepping the issue: shifting the focus to rules concerning the ongoing litigation would

39 Deeks, supra note 4, 304-305; N. Tsagourias and R. Buchan, Cyber-Threats and International Law, in M. E. Footer et al. (eds.), Security and International Law (2016), 365, 374.

40 On sovereignty and cyberspace, see generally W. Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 89 International Law Studies (2013), 123, 126; P. W. Franzese, Sovereignty in Cyberspace: Can it Exist?, 64 Air Force Law Review (2009), 1; B. Pirker, Territorial Sovereignty and Integrity and the Challenges of Cyberspace, in K. Ziolkowski, supra note 3, 189; M. Finnemore and D. B. Hollis, Constructing Norms for Global Cybersecurity, 110 American Journal of International Law (2016), 425, 459-460.

41 S. Chesterman, The Spy Who Came in From the Cold War: Intelligence and International Law, 27 Michigan Journal of International Law (2006), 1071, 1085-1086; J. Kish, International Law and Espionage (1995), 115-121; F. Lafouasse, L'espionnage dans le droit international (2012), 140-142. See however R. A. Falk, Space Espionage and World Order: A Consideration of the Samos-Midas Program, in R. J. Stanger (ed.), Essays on Espionage and International Law (1962), 45.

42 Schmitt, supra note 38, 170.

enable the adjudicator to put on record a violation of said rules without having to pass judgment on the actual act of ICT intelligence gathering.

At first blush, the duty not to aggravate or extend a dispute shows promise as a prism through which to assess cyber espionage. Citing case law,[43] treaty practice,[44] the UNGA's Friendly Relations Declaration[45] and good faith, the Arbitral Tribunal in the *South China Sea* case elevated its rank to that of a principle of international law applicable to parties involved in a procedure of dispute settlement for as long as that process lasts.[46] The arbitrators went on to describe in minute detail what it means to aggravate a dispute:

> In the course of dispute resolution proceedings, the conduct of either party may aggravate a dispute where that party continues during the pendency of the proceedings with actions that are alleged to violate the rights of the other, in such a way as to render the alleged violation more serious. A party may also aggravate a dispute by taking actions

---

43 In particular Electricity Company of Sofia and Bulgaria (Belgium v. Bulgaria), Interim Measures of Protection, Order, 1939, PCIJ Series A/B, No. 79, 199: "the principle universally accepted by international tribunals […] to the effect that the parties to a case must abstain from any measure capable of exercising a prejudicial effect in regard to the execution of the decision to be given and, in general, not allow any step of any kind to be taken which might aggravate or extend the dispute".

44 E.g. Revised General Act for the Pacific Settlement of International Disputes, 28 April 1949, Art. 33 (3), 71 UNTS 101: "The parties undertake to abstain from all measures likely to react prejudicially upon the execution of the judicial or arbitral decision or upon the arrangements proposed by the Conciliation Commission and, in general, to abstain from any sort of action whatsoever which may aggravate or extend the dispute".

45 Friendly Relations Declaration, supra note 21: "States parties to an international dispute, as well as other States shall refrain from any action which may aggravate the Situation so as to endanger the maintenance of international peace and security, and shall act in accordance with the purposes and principles of the United Nations".

46 South China Sea Arbitration, supra note 8, paras. 1166-1173. It is worthwhile noting that non-aggravation was explicitly written into the Rules of Procedure of the Timor-Leste-Australia Conciliation. See Conciliation between the Democratic Republic of Timor-Leste and the Commonwealth of Australia, PCA Case No. 2016-10, Rules of Procedure, Art. 10 (3): "The Parties shall refrain during the conciliation proceedings from any measure which might aggravate or widen the dispute. They shall, in particular, refrain from any measures which might have an adverse effect on proposals which are or may reasonably be made by the Commission, so long as those proposals have not been explicitly rejected by either of the Parties."

> that would frustrate the effectiveness of a potential decision, or render its implementation by the parties significantly more difficult. Finally, a party may aggravate a dispute by undermining the integrity of the dispute resolution proceedings themselves, including by rendering the work of a court or tribunal significantly more onerous or taking other actions that decrease the likelihood of the proceedings in fact leading to the resolution of the parties' dispute.[47]

There is little doubt that clandestine efforts to retrieve information from an opposing litigant could undercut the integrity of the proceedings resulting in further aggravation of the dispute. This alone however would not breach the duty, as the Arbitral Tribunal drew attention to an important restriction abridging its scope:

> [I]nternational law [does not] go so far as to impose a legal duty on a State to refrain from aggravating generally their relations with one another, however desirable it might be for States to do so. Actions must have a specific nexus with the rights and claims making up the parties' dispute in order to fall foul of the limits applicable to parties engaged in the conduct of dispute resolution proceedings.[48]

Consonant with the *South China Sea* award, covert ICT activities would only violate the aggravation prohibition to the extent that they bear a close relation to the subject-matter of the underlying dispute, something which can only be answered on a case-by-case basis.

At this juncture, we will focus on the communications between a State party to a dispute and its legal advisers. Are there solid grounds for granting attorney-client State correspondence juridical cover? The ICJ was called upon to solve this puzzle in the *Questions relating to the Seizure and Detention of Certain Documents and Data* case between Timor-Leste and Australia.[49] The facts of the case bear repeating. Proceedings were initiated by

---

47 South China Sea Arbitration, supra note 8, para. 1176.

48 Ibid., para. 1174.

49 Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, ICJ Reports 2014, 147. See also M. Happold, 'East Timor Takes Australia to ICJ over Documents Seized by Australian Intelligence' (2013), available at http://www.ejiltalk.org/east-timor-takes-australia-to-icj-over-documents-seized-by-australian-intelligence/ (last visited 23 October 2018); M. Happold, 'Timor Leste's Request for Provisional Measures: ICJ Orders Materials Seized by Australia Sealed Until Further Notice' (2014), available at http://www.ejiltalk.org/timor-lestes-request-for-provisional-measures-icj-orders-materials-seized-by-australia-sealed-until-further-notice/ (last visited 23 October

East Timor in December 2013 in response to a raid carried out by Australian intelligence services in the Australia-based business premises of a lawyer advising East Timor. At least some of the documents and data taken by the Australian authorities related to the then pending *Timor Sea Treaty Arbitration*[50] or potential maritime boundary negotiations. Said items concerned exchanges between East Timor and its legal advisers.[51] Together with the institution of proceedings, the applicant asked the Court to adopt provisional measures aimed at protecting the seized documents and ensuring the confidentiality of its contents.[52] The Timorese request for relief succeeded: the ICJ's Order indicated several measures that Australia had to adopt to protect the applicant's rights in the interim.[53] Per the parties' wishes, the ICJ later modified the measures,[54] then discontinued and removed the case from the list before any hearing on the merits could take place.[55]

2018); C. Rose, The Protection of Communications between States and their Counsel in International Dispute Settlement, 73 Cambridge Law Journal (2014), 231.

50 Arbitration under the Timor Sea Treaty (Timor-Leste v. Australia), PCA Case No. 2013-16. Incidentally, East Timor initiated this arbitration on the basis of allegations of Australian espionage. See K. Mitchell and D. Akande, 'Espionage & Good Faith in Treaty Negotiations: East Timor v. Australia' (2014), http://www.ejiltalk.org/espionage-fraud-good-faith-in-treaty-negotiations-east-timor-v-australia-in-the-permanent-court-of-arbitration/ (last visited 23 October 2018). These proceedings are distinct from the conciliation between East Timor and Australia under UNCLOS and another arbitration between the same parties concerning a petroleum export pipeline. See Timor-Leste-Australia Conciliation, supra note 46; Arbitration under the Timor Sea Treaty (Timor-Leste v. Australia), PCA Case No. 2015-42. Both arbitrations were terminated pursuant to the constructive dialogue within the framework of the conciliation. See 'Joint Statement by the Governments of Timor-Leste and Australia and the Conciliation Commission constituted pursuant to Annex V of the United Nations Convention on the Law of the Sea' (2017), https://pcacases.com/web/sendAttach/2049 (last visited 23 October 2018).

51 Seizure and Detention, supra note 49, para. 27.

52 East Timor further requested the President of the Court to exercise his powers under Article 74 (4) of the Rules of Court to call upon Australia to take certain immediate actions. Rules of Court, Art. 74 (4): "Pending the meeting of the Court, the President may call upon the parties to act in such a way as will enable any order the Court may make on the request for provisional measures to have its appropriate effects."

53 Seizure and Detention, supra note 49, para. 55.

54 Ibid., Order of 22 April 2015.

55 Ibid., Order of 11 June 2015.

East Timor's plea rested on a two-pronged strategy. Each part will be considered in turn with reflections being offered on their possible relevance to clandestine ICT activities. The applicant first advanced "the ownership and property rights which it holds over the seized material, entailing the rights to inviolability and immunity of this property (in particular, documents and data), to which it is entitled as a sovereign State".[56] In its Order indicating provisional measures, the Court left this part of East Timor's submissions unanswered, having already found the applicant's other rights to be plausible (as will be discussed later on). The most salient feature of East Timor's argumentation for our purposes is the assertion that over time various conventions and State practice have blended into "a customary rule of international law that grants immunity and inviolability to State documents and archives".[57] Had the case proceeded on the merits, this novel take on property might not have swayed the judges. As counter-intuitive as it may seem, States do not enjoy a universal right to property under contemporary international law.[58] Property rights have developed in a fragmentary manner whereby protection is bestowed on well-defined categories of objects such as spacecraft, aircraft and ships.[59]

The flipside is that when they do apply, specialized legal regimes can provide that sought-after safeguard. For instance, if the targeted exchanges were between the legal advisors and a diplomatic mission of the client State and/or were exfiltrated from an embassy's premises, the interception is likely to have breached diplomatic law. The violation stems from the diplomatic mission's premises, archives, documents and official correspondence being inviolable under the VCDR and customary international law.[60] Although crafted in an era preceding the digital revolution, the relevant terms of the VCDR extend to official correspondence stored and sent electronically.[61]

---

56 Ibid., Provisional Measures, para. 24.

57 Ibid., Memorial of Timor-Leste (2014), 48.

58 P. Tzeng, The State's Right to Property Under International Law, 125 Yale Law Journal (2016), 1805.

59 Ibid., 1809-1811.

60 VCDR, supra note 27, Articles 22 (1), 24 and 27 (2). United States Diplomatic and Consular Staff in Tehran, supra note 12, paras. 62, 69. There is some debate on whether the duty to respect the inviolability of the sending State in this regard is only incumbent upon the receiving State or extends to third States as well. See Schmitt, supra note 38, 214, 221-222.

61 P. Grané Labat and N. Burke, The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention?, in P. Behrens (ed.), Diplomatic Law in a New Millennium (2017), 204; W.-M. Choi, Diplomatic and

Secondly, Timor-Leste requested protection for what it called "the right to the confidentiality of communications with its legal advisers".[62] Notwithstanding Australia's national security concerns[63] and tendered assurances, the Court was receptive to the applicant's submission in holding that:

> If a State is engaged in the peaceful settlement of a dispute with another State through arbitration or negotiations, it would expect to undertake these arbitration proceedings or negotiations without interference by the other party in the preparation and conduct of its case. It would follow that in such a situation, a State has a plausible right to the protection of its communications with counsel relating to an arbitration or to negotiations, in particular, to the protection of the correspondence between them, as well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context.[64]

Pursuant to this dictum, the ICJ ordered Australia not to interfere in communications between East Timor and its legal advisers in relation to the pending arbitration and maritime delimitation negotiations.[65]

The above passage lends itself well to the cyber context. Based on a plain reading of the Court's language, mainly the words "communications", "correspondence" and "data", the present author sees no obstacle to interpreting its scope so as to include digital exchanges such as e-mails. The fact that the seized items in *Timor-Leste v. Australia* included electronically stored data strengthens this understanding. That said, the Court's holding is not free of all ambiguity. To begin with, this is not the final say on the protection of attorney-client correspondence under international law given that it comes from an order indicating provisional measures. When exercising this form of incidental jurisdiction the Court solely has to determine whether the

---

Consular Law in the Internet Age, 10 Singapore Year Book of International Law (2006), 117. See also R (Bancoult) v. Secretary of State for Foreign and Commonwealth Affairs (No. 3) [2013] EWHC 1502 (Admin): "We have no doubt that the context, object and purpose of the 1961 Convention require the words 'document' and 'correspondence' to include modern forms of electronic communication with the possible exception of communication by voice only. Likewise, an electronic storage system of such communications is an 'archive'".

62 Seizure and Detention, supra note 49, Provisional Measures, para. 24.

63 See S. Tully, Legal Professional Privilege and National Security, 30 Bar News: The Journal of the New South Wales Bar Association (2014), 24.

64 Seizure and Detention, supra note 49, Provisional Measures, para. 27.

65 Ibid., para. 55.

rights for which the applicant seeks protection are *plausible*, not definite.[66] With the case having ended before reaching the merits stage, the ICJ will not have the opportunity to conclusively confirm (or repudiate) its tentative position.

The basis in international law for shielding a State's communications with its legal advisers raises further uncertainty. The Court held that it:

> Might be derived from the principle of the sovereign equality of States, which is one of the fundamental principles of the international legal order and is reflected in Article 2, paragraph 1, of the Charter of the United Nations. More specifically, equality of the parties must be preserved when they are involved, pursuant to Article 2, paragraph 3, of the Charter, in the process of settling an international dispute by peaceful means.[67]

Indeed, the duty to peacefully resolve disputes can be undermined when one party gains access to another party's privileged communications when both are locked in litigation.[68] The drawback however lies not with the rationale but with the method. The Court extracts a very concrete right of confidentiality from very broad UN Charter principles. If anything, this is innovative and the bench presents neither State practice, nor *opinio juris* or jurisprudence to bolster its reasoning.[69] Perhaps that is what led two judges to question the majority's reliance on the UN's founding document as the building block for the right of non-interference.[70]

Recourse to general principles of law[71] rather than treaty or custom offers a viable alternative. The latter denote unwritten, wide-ranging legal

---

66 C. A. Miles, Provisional Measures before International Courts and Tribunals (2017), 193-201.

67 Seizure and Detention, supra note 49, Provisional Measures, para. 27. On the equality of States in proceedings before the ICJ, see M. Bedjaoui, L'Egalité des Etats dans le procès international, un mythe?, in Liber amicorum Jean-Pierre Cot: Le procès international (2009), 1-27.

68 Although the putative right is discussed in relation to arbitration and negotiation, there is no reason why it would not apply to any other means of the parties' choosing, for instance judicial settlement.

69 R. J. Bettauer, Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia). Provisional Measures Order, 108 American Journal of International Law (2014), 763, 768-769.

70 Seizure and Detention, supra note 49, Provisional Measures, Dissenting Opinion of Judge Greenwood, para. 12; Ibid., Separate Opinion of Judge Donoghue, para. 18.

71 ICJ Statute, Art. 38 (1) (c).

norms which (a) enjoy recognition in the municipal legal systems of States (*in foro domestico*) and (b) are transposable to the international plane.[72] It has been argued – including by East Timor[73] – that attorney-client (or legal professional) privilege is a general principle of law. This norm, which "promote[s] open and candid communications between lawyer and client and thereby further[s] the administration of justice"[74] is found in a great many jurisdictions across the world in one shape or another, so the *in foro domestico* criterion is easily met.[75] Moving to the next requirement, certain principles of domestic law are ill-adapted to "conditions in the international field"[76] and for that reason cannot be transposed to international law. By way of illustration, the notion of compulsory jurisdiction, the hallmark of municipal courts, cannot constitute a general principle of law as it would clash with the consensual model of international adjudication.[77] Legal professional privilege does not have to contend with comparable hurdles. There is therefore little reason why it cannot be implemented in the international arena to the benefit of attorney-client State correspondence. The case law of international courts and tribunals points in the same direction.[78] The Arbitral Tribunal in the *Bank for International Settlements* case offered one of the most significant pronouncements to date:

> At the core of the attorney-client privilege in both domestic and international law is the appreciation that those who must make decisions on their own or others' behalf are entitled to seek and receive legal advice and that the provision of a full canvass of legal options and the exploration and evaluation of their legal implications would be chilled, were counsel and their clients not assured in advance that the advice

72 A. Pellet, Article 38, in Zimmermann, supra note 11, 731, 834.
73 Seizure and Detention, supra note 49, Provisional Measures, para. 24; Ibid., Memorial of Timor-Leste (2014), 52-57.
74 A. Möckesch, Attorney-Client Privilege in International Arbitration (2017), 124.
75 Ibid., 222; R.M. Mosk and T. Ginsburg, Evidentiary Privileges in International Arbitration, 50 International and Comparative Law Quarterly (2001), 345, 378-379.
76 Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain) (New Application: 1962), Judgment, Separate Opinion of Judge Fitzmaurice, ICJ Reports 1970, para. 5.
77 Status of Eastern Carelia, Advisory Opinion, 1923, PCIJ Series B, No. 5, 27: "It is well established in international law that no State can, without its consent, be compelled to submit its disputes with other States either to mediation or to arbitration, or to any other kind of pacific settlement"; Pellet, supra note 72, 840-841.
78 Seizure and Detention, supra note 49, Memorial of Timor-Leste (2014), 52-57.

> proffered, along with communications related to it, would remain confidential and immune to discovery.[79]

Turning to investor-State dispute settlement, the *Libananco* case gained notoriety for the applicant's charge that it had come under surveillance and interception by the host State. Treating the matter "with the utmost seriousness", the tribunal proclaimed that the allegations struck at "fundamental principles", including "respect for confidentiality and legal privilege" and "the right of parties both to seek advice and to advance their respective cases freely and without interference".[80] Peering beyond the world of arbitration, standing bodies such as the Court of Justice of the European Union[81] and the European Court of Human Rights[82] have shown like concern for the preservation of the principle. Although the precedents discussed thus far do not specifically address the confidentiality between a client *State* – as opposed to clients in general – and its legal advisers, they do stand for the proposition that legal professional privilege forms part and parcel of international law.[83]

---

79 Bank for International Settlements, Procedural Order No. 6 of 11 June 2002, PCA Case No. 2000-04, 10. See also Vito G. Gallo v. Government of Canada, Procedural Order No. 3 of 8 April 2009, PCA Case No. 2008-02, para. 49.

80 Libananco Holdings Co. Limited v. Turkey, Decision on Preliminary Issues of 23 June 2008, ICSID Case No. ARB/06/8, paras. 74, 78.

81 AM & S Europe Limited v. Commission of the European Communities, ECLI:EU:C:1982:157, Judgment of 18 May 1982, para. 21: "there are to be found in the national laws of the Member States common criteria inasmuch as those laws protect, in similar circumstances, the confidentiality of written communications between lawyer and client […]".

82 In a case involving the seizure of electronically stored data, the Strasbourg Court stated: "While there is nothing in the facts to suggest that papers covered by legal professional privilege were touched upon during the search, it should be noted that the police removed the applicant's entire computer, including its peripherals, as well as all floppy disks which they found in his office [...]. Seeing that the computer was evidently being used by the applicant for his work, it is natural to suppose that its hard drive, as well as the floppy disks, contained material which was covered by legal professional privilege." Iliya Stefanov v. Bulgaria, ECtHR Application No. 65755/01, Judgment of 22 May 2008, para. 42.

83 G. Giraudeau, À propos de l'affaire des Questions concernant la saisie et la détention de certains documents et données (Timor-Leste c. Australie): Quand la Cour internationale de Justice protège les droits d'un Etat partie à une autre instance, 61 Annuaire français de droit international (2015), 239, 258-260.

Determining the scope of legal professional privilege in international law serves as a reminder that the devil lies always in the detail.[84] For one, attorney-client privilege is not absolute; exceptions exist because a balance is struck between confidentiality and competing values such as accurate judicial fact-finding and the imperatives of law enforcement. Countries weigh these interests differently; accordingly the rule's protective reach will differ from one jurisdiction to the next. Other features, e.g. who may waive the privilege and what types of information are covered, also vary considerably.[85] The extent of the limitations placed on privilege in the inter-State context cannot be conclusively answered at this stage lacking additional jurisprudential development.[86] However, the *Seizure and Detention* case does hint at the inter-State principle being far less restricted than the municipal equivalent of legal professional privilege.[87] The Court suggested as much when it directed Australia not to interfere "in any way" in East Timor's communications with its lawyers in relation to the pending arbitration and maritime boundary negotiations.[88] This measure, which does not mention potential exceptions, was adopted by an overwhelming majority of 15-1 even with Australia's national security concerns, criminal investigations, and the written guarantees presented by the Australian Attorney-General himself to the Court.[89] At a minimum, there are robust reasons for con-

84 Interestingly, the Australian-appointed judge ad hoc in the case brought by East Timor before the ICJ did not outright deny the existence of such a norm in international law, observing instead that "[t]he extent to which there is a settled principle of legal professional privilege, unique to the law of nations, and immune to any limitation in an international or national interest, will require detailed and careful argument." Seizure and Detention, supra note 49, Provisional Measures, Dissenting Opinion of Judge ad hoc Callinan, para. 26.

85 Möckesch, supra note 74, 221-223.

86 See M. T. Grando, An International Law of Privileges, 3 Cambridge Journal of International and Comparative Law (2014), 666, 686-695 (on how public international tribunals should decide claims of privilege and balance the relevant social policies).

87 G. Giraudeau, 'The Principles of Confidentiality and Noninterference in Communications with Lawyers and Legal Advisers in Recent ICJ and ECHR Case Law' (2016), available at https://www.asil.org/insights/volume/20/issue/16/principles-confidentiality-and-noninterference-communications-lawyers (last visited 23 October 2018). On recent ECtHR jurisprudential developments, see M. Moris, Le secret professionnel de l'avocat au regard de l'article 8 de la Convention européenne des droits de l'homme. De nouveaux enseignements de la Cour de Strasbourg, 113 Revue trimestrielle des droits de l'homme (2018), 179.

88 Seizure and Detention, supra note 49, Provisional Measures, para. 55 (3).

89 Giraudeau, supra note 87. See also Bettauer, supra note 69, 767.

cluding that in clear-cut cases, such as the interception of e-mail exchanges between a State and its legal adviser related to proceedings before an international court or arbitral tribunal, the responsible State has fallen short of its obligations.

IV. Evidence Procured through Cyber Espionage: Too Hot to Handle?

It is conceivable that a party that has been spied on would seek cessation of the case for betrayal of trust. The probability of a tribunal agreeing to a unilateral request of this nature will oftentimes be slim. The *Croatia/Slovenia* arbitration, mentioned in the introduction to this contribution, is instructive. In the wake of the revelation that Slovenia's agent and party-appointed arbitrator had partaken in *ex parte* communications, Croatia sought termination of the Arbitration Agreement. The Tribunal in its new composition examined and rejected the petition but not without putting on record Slovenia's unlawful behaviour. In the arbitrators' estimation, the Slovenian breach had not made the continuation of the case impossible and, thus, the object and purpose of the Agreement had not been defeated.[90] Inspired by this precedent, an international court or tribunal could similarly issue a declaratory ruling against the spying litigant, all the while letting the case proceed.

Instead of bringing proceedings to an abrupt end, adjudicators could avail themselves of less drastic courses of action. The indication of provisional measures comes to mind. Safeguarding the proper conduct of the proceedings, explicitly recognized in certain statutes as a ground for granting interim measures,[91] could prompt an injunction ordering a litigant to refrain from further acts of intelligence gathering targeting the other party. Attaching financial consequences to the inappropriate behaviour could be contemplated as well.[92]

---

90 Croatia v. Slovenia, supra note 14.

91 E.g. ECtHR Rules of Court, Rule 39 (1).

92 A differentiated allocation of costs might constitute an appropriate sanction. See Croatia v. Slovenia, supra note 14, paras. 229-230: "Finally, the Tribunal observes that the events that have given rise to the present Partial Award have significantly increased the costs of the present proceedings. If these events had not occurred, the advances toward the costs of arbitration that both Parties have made would have sufficed until the rendering of a final award in these proceedings. It is evident that, under the present circumstances, further advances will be required. […] While the Tribunal reserves its position on the ultimate allocation of costs in these proceedings until its final award, it considers that, for the time being, it is appro-

This section will focus on yet another option, i.e. the disregarding of evidence that has been acquired through clandestine ICT intelligence gathering. Unlike domestic national courts of the common law tradition, bound to apply a web of technical exclusionary rules, inter-State tribunals are not weighed down by that level of restriction.[93] Arbitral rules tend to give international arbitrators free reign when it comes to the admissibility of evidence.[94] What then is to be made of illegally obtained evidence? To reiterate: there is good reason to believe that spying, including through digital means, is at odds with the law of international dispute settlement. By extension, the intrusion into international proceedings of evidence surreptitiously procured through computer networks raises understandable concern. Ample cause, therefore, to recast an old debate in a new cyber age.

Some have argued that the exclusion of unlawfully acquired evidence might be a general principle of law given its presence in national legal systems.[95] Taking a more cautious tack, others have drawn analogies from the municipal realm without going so far as to claim discovery of a new general principle.[96] Either view has its shortcomings. The generality of the rule

priate that Slovenia shall advance the sums necessary to cover costs that arise as a result of the prolongation of the proceedings beyond the originally envisaged timetable."; Ahmadou Sadio Diallo (Republic of Guinea v. Democratic Republic of the Congo), Compensation, Judgment, ICJ Reports 2012, para. 60: "The Court recalls that Article 64 of the Statute provides that, '[u]nless otherwise decided by the Court, each party shall bear its own costs'. While the general rule has so far always been followed by the Court, Article 64 implies that there may be circumstances which would make it appropriate for the Court to allocate costs in favour of one of the parties."

93 There are very few exclusionary rules applicable to the ICJ or ITLOS, the inadmissibility of evidence from negotiations between the parties being the main one. Factory at Chorzów (Germany v. Poland), Merits, Judgment, 1928, PCIJ Series A, No. 17, 51: "the Court cannot take into account declarations, admissions or proposals which the Parties may have made during direct negotiations between themselves, when such negotiations have not led to a complete agreement." See further C. F. Amerasinghe, Evidence in International Litigation (2005), 163-167; M. Benzing, Evidentiary Issues, in Zimmermann, supra note 11, 1234, 1242-1245.

94 E.g. B. W. Daly et al., A Guide to the PCA Arbitration Rules (2014), 107.

95 R. Wolfrum and M. Möldner, International Courts and Tribunals, Evidence, in Wolfrum, supra note 18, para. 60.

96 W. M. Reisman and E. E. Freedman, The Plaintiff's Dilemma: Illegally Obtained Evidence and Admissibility in International Adjudication, 76 American Journal of International Law (1982), 737.

is dubitable for it appears to be a peculiarity of United States criminal law.[97] The analogy breaks down when one realizes that the *ratio* of the rule is to rein in overzealous criminal prosecution. To equate litigants in State-to-State proceedings with public prosecutors is to compare apples with oranges.[98]

The notion of there being hard-and-fast rules requiring the exclusion of improperly obtained evidence has not gained traction in international jurisprudence.[99] On this issue, the *Corfu Channel* case between the United Kingdom and Albania is the classic ruling most commentators gravitate towards. The underlying dispute arose from an incident that saw Royal Navy ships strike mines during their passage through the narrow Corfu Channel. In the aftermath of the event, the UK launched Operation Retail, a minesweeping mission which took place in Albanian waters without the coastal State's assent. The British defended their action *inter alia* on the basis of a so-called right of intervention to "secure possession of evidence in the territory of another State, in order to submit it to an international tribunal and thus facilitate its task".[100] Unconvinced by the argument, the bench condemned the UK's conduct as a "manifestation of a policy of force".[101] While the Court ruled out self-help through intervention for the purpose of collecting and preserving evidence, it appeared to rely on the information gleaned from Operation Retail.[102] An important fact to emphasize is that Albania did not actively challenge the use of evidence collected during the minesweeping. The takeaway from *Corfu Channel* is that the illegal circumstances in which evidence was obtained *might* bar its ad-

97 H. Thirlway, Dilemma or Chimera? – Admissibility of Illegally Obtained Evidence in International Adjudication, 78 American Journal of International Law (1984), 622, 627. On the risks of importing one's preferred municipal legal concepts into international law, see M. Benatar, International Law, Domestic Lenses, 3 Cambridge Journal of International and Comparative Law (2014), 357, 374-376.

98 Thirlway, supra note 97, 628-630.

99 A. Lagerwall, Le principe ex injuria jus non oritur en droit international (2016), 197-209.

100 Corfu Channel (United Kingdom v. Albania), Judgment, Merits, ICJ Reports 1949, 34.

101 Ibid., 35.

102 N. Hasan Shah, Discovery by Intervention: The Right of a State to Seize Evidence Located within the Territory of the Respondent State, 53 American Journal of International Law (1959), 595, 606-610.

missibility but in any event it is up to the parties to raise that objection.[103] To this day, the ICJ has never declared evidence procured through an internationally wrongful act inadmissible.[104] Applied to spying through ICT technology, digital evidence unlawfully taken from servers located in another State would not be deemed inadmissible on grounds of its illicit provenance alone.[105]

In 2010-2011, the international NGO WikiLeaks released a large batch of classified US diplomatic telegrams into the public domain (so-called 'Cablegate').[106] Parties to international legal proceedings have relied on cables from the leak as evidence. The development raises a question mark over the need or desire to disregard the contents of privileged diplomatic correspondence and archives that have been impermissibly acquired and disclosed by third parties.[107]

It has been reported that in an ICJ case between the former Yugoslav Republic of Macedonia (FYROM) and Greece, the Registrar deleted a reference to an uncovered diplomatic cable from the copy of pleadings distributed to the President and interpreters before the hearings were held.[108] The transcripts of the oral proceedings include footnote references to a cable from the US Embassy in London to the US State Department in the

---

103 R. Rivier, La preuve devant les juridictions interétatiques à vocation universelle (CIJ et TIDM), in H. Ruiz Fabri and J.-M. Sorel (eds.), La preuve devant les juridictions internationales (2007), 9, 34-35.

104 A. Riddell and B. Plant, Evidence before the International Court of Justice (2009), 155.

105 M. Roscini, Digital Evidence as a Means of Proof before the International Court of Justice, 21 Journal of Conflict and Security Law (2016), 541, 551-554; M. Roscini, Evidentiary Issues in International Disputes Related to State Responsibility for Cyber Operations, 50 Texas International Law Journal (2015), 233, 269-272.

106 WikiLeaks, 'Public Library of US Diplomacy', available at https://wikileaks.org/plusd/about/#cab (last visited 23 October 2018).

107 Grané Labat and Burke, supra note 61, 225-227, 229-230. On the (attempted) use of WikiLeaks cables as evidence in international and municipal proceedings, see C. Blair and E. Vidak Gojković, WikiLeaks and Beyond: Discerning an International Standard for the Admissibility of Illegally Obtained Evidence, 33 ICSID Review (2018), 235; E. Carpanelli, On the Inviolability of Diplomatic Archives and Documents: The 1961 Vienna Convention on Diplomatic Relations to the Test of WikiLeaks, 98 Rivista di diritto internazionale (2015), 834; R. McCorquodale, 'Wikileaks Documents are Admissible in a Domestic Court' (2018), available at https://www.ejiltalk.org/wikileaks-documents-are-admissible-in-a-domestic-court/ (last visited 23 October 2018).

108 Grané Labat and Burke, supra note 61, 226.

pleadings read out by counsel to FYROM.[109] The ICJ's Judgment does not mention any sources revealed by WikiLeaks.

The *Chagos Marine Protected Area* Arbitration initiated by Mauritius against the UK pursuant to Annex VII of UNCLOS sought to invalidate a marine protected area established around the British Indian Ocean Territory (Chagos Archipelago).[110] The decision to bring the case was in part influenced by a diplomatic cable leaked via WikiLeaks. The cable contained a report of an alleged meeting between US and UK officials demonstrating ulterior, non-environmental motives for declaring the marine park.[111] The very same cable had already surfaced in the *Bancoult* litigation before British courts which dealt with the eviction and resettlement of the archipelago's inhabitants.[112] Noting that the document "appears to have been obtained illicitly by a person who was not authorised to obtain it", the UK invoked the VCDR rules enshrining the inviolability of the archives, documents and official correspondence of the diplomatic mission.[113] The Annex VII Arbitral Tribunal held that it "had reviewed the record of the English court proceedings that considered the matter and sees no basis to question the conclusion reached following the examination of the relevant individuals, that the content of that meeting was not as recorded in the leaked cable. Nor does the Tribunal consider it appropriate to place weight on a record of such provenance".[114] This language implies that the arbitrators' unwillingness to use the WikiLeaks source was due to its dubious probative value and not merely how it made its way into the public domain.[115]

Investor-State dispute settlement has also been the scene of (attempted) uses of evidence from classified diplomatic communications. The results have been mixed.[116] The respondent in *ConocoPhillips v. Venezuela* submitted sources from Cablegate as part of new evidence justifying its challenge

---

109 Application of the Interim Accord of 13 September 1995 (the former Yugoslav Republic of Macedonia v. Greece), CR 2011/6 of 22 March 2011, 30, footnote 44 and 57, footnote 108, available at http://www.icj-cij.org/ (last visited 23 October 2018).

110 Chagos Marine Protected Area Arbitration (Mauritius v. United Kingdom), Award of 18 March 2015, PCA Case No. 2011-03.

111 Ibid., paras. 494, 497.

112 Grané Labat and Burke, supra note 61, 219-223.

113 Chagos, supra note 110, Counter-Memorial of the United Kingdom (2013), para. 8.64, footnote 730.

114 Chagos, supra note 110, Award of 18 March 2015, para. 542.

115 Grané Labat and Burke, supra note 61, 227.

116 J. O. Ireton, The Admissibility of Evidence in ICSID Arbitration: Considering the Validity of WikiLeaks Cables as Evidence, 30 ICSID Review (2015), 231.

to an earlier ruling of the ICSID Tribunal. The investor questioned the admissibility and relevance of the cables but not the accuracy of their contents. By two votes to one, the panel found that it lacked the power to reconsider its previous decision and for that reason did not examine the evidence.[117] The dissenting arbitrator, who described the cables as "chang[ing] the situation radically in dimension and seriousness" and having "a high degree of credibility", disagreed strongly with the majority's reasoning.[118] The Tribunal issued an Interim Decision in early 2017 that did scrutinize the leaked cables but concluded that they did not support the respondent's allegations.[119] In other ICSID arbitrations where WikiLeaks cables were presented, the adjudicators did not comment on their admissibility and propriety nor did the opposing parties object to their admission. The panels failed to consider the cables in these cases.[120] Conversely, the Arbitral Tribunal hearing claims brought by Yukos shareholders, constituted in accordance with the Energy Charter Treaty, did employ WikiLeaks sources in its analysis of the evidentiary record.[121] Taking stock of the (non-)treatment of WikiLeaks sources in international case law, little support can be found for the notion that illegally obtained evidence must be cast aside (even if that would be desirable on policy grounds).[122]

The surveyed international precedents do not contradict the overall approach to fact-finding predicaments. On the whole, courts have preferred

---

117 ConocoPhillips Petrozuata BV, ConocoPhillips Hamaca BV and ConocoPhillips Gulf of Paria BV v. Bolivarian Republic of Venezuela, Decision on Respondent's Request for Reconsideration of 10 March 2014, ICSID Case No. ARB/07/30.

118 Ibid., Dissenting Opinion of Georges Abi-Saab, para. 64.

119 ConocoPhillips v. Venezuela, supra note 117, Interim Decision of 17 January 2017, paras. 117-126 and 135.

120 Ireton, supra note 116, 240; OPIC Karimum Corporation v. Bolivarian Republic of Venezuela, Decision on the Proposal to Disqualify Professor Philippe Sands, Arbitrator of 5 May 2011, ICSID Case No. ARB/10/14, paras. 11, 23, 56-57; Kiliç İnşaat İthalat İhracat Sanayi Ve Ticaret Anonim Şirketi v. Turkmenistan, Award of 2 July 2013, ICSID Case No. ARB/10/1, paras. 4.3.16, 8.1.10 and 8.1.21.

121 Hulley Enterprises Limited (Cyprus) v. The Russian Federation, Final Award of 18 July 2014, PCA Case No. 2005-03/AA226, paras. 1186, 1189, 1199, 1201, 1208, 1213 and 1223; Yukos Universal Limited (Isle of Man) v. The Russian Federation, Final Award of 18 July 2014, PCA Case No. 2005-04/AA227, paras. 1186, 1189, 1199, 1201, 1208, 1213 and 1223; Veteran Petroleum Limited (Cyprus) v. The Russian Federation, Final Award of 18 July 2014, PCA Case No. 2005-05/AA228, paras. 1186, 1189, 1199, 1201, 1208, 1213 and 1223.

122 Grané Labat and Burke, supra note 61, 227 (advocating the inadmissibility of leaked diplomatic documentation as evidence because it would further the proper functioning of diplomatic missions).

to walk the well-trodden path of circumvention: a deft reframing of the *ratio decidendi* will avoid having to consider contested evidence as part of the factual basis of the ruling.[123] A striking resemblance can be found with the way in which international tribunals have handled fraudulent evidence.[124]

As we ponder this state of affairs, it is worth considering whether *de lege ferenda* a principled approach to the use of tainted evidence should and could prevail. That adjudicators are disinclined to spurn documentation submitted by States is an understandable corollary of sovereignty.[125] Nonetheless, undue deference of an international court to the sovereignty of clients should not come at the expense of proper control over its procedural system.[126] Maybe justice is best served when the fruit of espionage is struck from the record or disregarded on pertinent policy grounds rather than solely on a legal/illegal binary logic. Exploring the terrain that lies beyond pure inter-State adjudication pays dividends. In a 2017 study on due process in transnational arbitration, the authors remarked that "[i]t should come as no surprise—based on previous discussions of good faith, procedural equality, and fraud—that *proof acquired by unlawful or otherwise improper means may be stricken out from the record or denied any weight*".[127] The conclusion was reached largely on the strength of the NAFTA Tribunal's reasoning in the *Methanex* case. The Tribunal held that:

> As a general principle, therefore, just as it would be wrong for the USA ex hypothesi to misuse its intelligence assets to spy on Methanex (and its witnesses) and to introduce into evidence the resulting materials into this arbitration, so too would it be wrong for Methanex to introduce evidential materials obtained by Methanex unlawfully.

123 B. Kingsbury, International Courts: Uneven Judicialisation in Global Order, in J. Crawford and M. Koskenniemi (eds.), The Cambridge Companion to International Law (2012), 203, 220.

124 W. M. Reisman and C. Parajon Skinner, Fraudulent Evidence before Public International Tribunals: The Dirty Stories of International Law (2014), 197-198.

125 Riddell and Plant, supra note 104, 151.

126 R. Higgins, Respecting Sovereign States and Running a Tight Courtroom, 50 International and Comparative Law Quarterly (2001), 121.

127 C. T. Kotuby and L. A. Sobota, General Principles of Law and International Due Process: Principles and Norms Applicable in Transnational Disputes (2017), 196-197. See also Blair and Vidak Gojković, supra note 107, 256-258 (proposing a three-step test for determining the admissibility of evidence of illegal origin).

and

> […] the Tribunal likewise decided that it 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.[128]

Let us also revisit the *Libananco* arbitration for good measure. Reacting to alarming allegations of surveillance directed at the applicant, the ICSID Tribunal stated categorically that it had:

> no doubt for a moment that, *like any other international tribunal, it must be regarded as endowed with the inherent powers required to preserve the integrity of its own process* […]. The Tribunal would express the principle as being that parties 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; this principle applies in all arbitration, including investment arbitration, and to all parties, including States (even in the exercise of their sovereign powers).[129]

Procedural integrity[130] would indeed make a fitting benchmark against which to test the admission of documentation obtained through unauthorized access to another State's databases. Better yet, linking integrity of proceedings to admissibility of evidence is not without antecedent. Although treated as fundamentally distinct from inter-State adjudication (and rightly so), international criminal tribunals can sometimes serve as a source of inspiration for international dispute settlement procedures.[131] The Rules of

---

128 Methanex Corporation v. United States of America, Final Award of 3 August 2005, NAFTA, 44 International Legal Materials (2005), 1345, paras. 54, 59. Taking its cue from the Methanex award, the Tribunal in EDF v. Romania declared inadmissible a secret audio recording, referring to "the principles of good faith and fair dealing required in international arbitration". EDF (Services) Limited v. Romania, Procedural Order No. 3 of 29 August 2008, ICSID Case No. ARB/05/13, para. 38.

129 Libananco v. Turkey, supra note 80, para. 78 (emphasis added).

130 Sarvarian, supra note 11, 9-10 (defining procedural integrity as a set of fair trial principles that includes the submission of evidence).

131 See e.g. Seizure and Detention, supra note 49, Provisional Measures, Separate Opinion of Judge Cançado Trindade, para. 39 (referring to the Blaškić case (ICTY) in order to reject a party having just cause to withhold documents on "national security" grounds).

Procedure and Evidence of the Mechanism for International Criminal Tribunals contains a provision to the effect that "[n]o evidence shall be admissible if obtained by methods which cast substantial doubt on its reliability or if its admission is antithetical to, and would seriously damage, the integrity of the proceedings".[132] An analogous clause in the inter-State context would allow international tribunals to move beyond an interminable debate on the legality of cyber espionage whilst mitigating its impact in the higher interests of the case unfolding before them.

V. Concluding Remarks

Guerrilla tactics in international litigation have been described as unconventional, unethical means which always derail proceedings but do not necessarily violate law or written rules of procedure in each and every instance.[133] It is hardly a stretch to add cyber espionage to this unsavoury list. This chapter has argued that in certain cases ICT intelligence gathering conducted in relation to proceedings before an international tribunal is prohibited by several rules regulating international dispute settlement. This finding can be reached without having to tackle spying under general international law, thereby providing judges and arbitrators hearing disputes between States with a practical tool and incentive to take a principled stand.

The picture is not altogether rosy. The case law and practice of inter-State litigation does not suggest total preparedness to deal with the ramifications of spying through digital means. The permissive attitude towards illicitly obtained evidence attests to that trend. Should such behaviour be countenanced or must a price be paid for having "polluted the proceedings"?[134] A major theme that has emerged throughout the pages of this piece is that if we venture beyond the confines of State-to-State dispute settlement, we can find useful practice on how this matter could be handled.

---

132 Rules of Procedure and Evidence of the Mechanism for International Criminal Tribunals, Rule 117, UN Doc. MICT/1/Rev. 2 (2016). See also Amerasinghe, supra note 93, 179-180.

133 R. Pfeiffer and S. Wilske, Introduction to Guerrilla Tactics in International Arbitration, in G. J. Horvath and S. Wilske (eds.), Guerrilla Tactics in International Arbitration (2013), 1, 3.

134 This phrase is borrowed from M/V "Louisa" (Saint Vincent and the Grenadines v. Spain), Judgment, Separate Opinion of Judge Cot, ITLOS Reports 2013, paras. 39, 79.

The strategies pursued by their fellow adjudicators provide inter-State courts and tribunals with much needed food for thought as an era of cyber espionage might be dawning upon them.