Bench Memorandum

Case Concerning the Suthan Referendum

Version 2

18 March 2022

***** CONFIDENTIAL*****

Only for use by Appointed Judges of the 2022 Philip C. Jessup International Law Moot Court Competition

IMPORTANT INFORMATION REGARDING THE BENCH MEMORANDUM

The Bench Memorandum is a confidential document that may be read only by judges and administrators of the Jessup Competition. Every possible measure must be taken to maintain the confidentiality of the Bench Memorandum, including compliance with the following guidelines:

- **Do not leave copies of the Bench Memorandum lying in public places.**
- **Do not, under any circumstance, discuss the Bench Memorandum or its contents with anyone other than judges and administrators.**
- **Do not, under any circumstance, distribute the Bench Memorandum to team members or team advisors, even after the regional or national competition that you have judged is over.**

If you have received this Bench Memorandum, you are no longer eligible to assist a team in any manner, including as a judge for practice oral rounds. Doing so could result in the disqualification of the team from the competition. See Official Rule 2.14.

The contents of the Bench Memorandum will remain confidential until the conclusion of the International Rounds in April 2022.

The Bench Memorandum is an evolving document. As the competition season progresses, new versions of the Bench Memorandum may become available. ILSA encourages judges and competition staff to make sure that they possess the most recent version of the Bench Memorandum.

ILSA welcomes comments and recommendations on the Bench Memorandum. Please send all suggestions to jessup@ilsa.org.

1. TABLE OF CONTENTS

1. TABLE OF CONTENTS 3
2. Purpose of the Bench Memorandum 5
3. Executive Summary 6
4. Preliminary Matters 8
   4.1 Jurisdiction 8
   4.2 Claims and Counterclaims 8
      4.2.1 Suggested Questions 8
5. QP1: Admissibility of Evidence 9
   5.1 Introduction 9
   5.2 Were the Documents Obtained in Breach of the VCDR? 10
      5.2.1 Applicant Arguments 10
      5.2.2 Respondent Arguments 11
      5.2.3 Suggested Questions 11
   5.3 Exclusion of the Documents Obtained from the Briefcase 12
      5.3.1 Applicant Arguments 12
      5.3.2 Respondent Arguments 14
      5.3.3 Suggested Questions 15
   5.4 Admissibility of the Conciliation Transcript/Recording 16
      5.4.1 Applicant Arguments 16
      5.4.2 Respondent Arguments 17
      5.4.3 Suggested Questions 17
6. QP2: Election Interference 18
   6.1 Introduction 18
   6.2 Attribution of SAD's Misinformation Campaign 18
      6.2.1 Applicant Arguments on Art 8 ARSIWA 19
      6.2.2 Respondent Arguments on Art 8 ARSIWA 20
      6.2.3 Applicant Arguments on Art 11 ARSIWA 20
      6.2.4 Respondent Arguments on Art 11 ARSIWA 21
      6.2.5 Suggested Questions 22
   6.3 Legality of SAD's Misinformation Campaign 22
      6.3.1 Applicant Arguments on Non-Intervention 23

6.3.2 Applicant Arguments on Sovereignty 24
6.3.3 Respondent Arguments on Non-Intervention 25
6.3.4 Respondent Arguments on Sovereignty 26
6.3.5 A Note on the Principle of Self-Determination 26
6.3.6 A Note on Funding by the Ravarian Embassy and Art 41 VCDR 27
6.3.7 Suggested Questions 27
7. QP3: Suspension of Hunland's Pano Account 28
7.1 Introduction 28
7.2 Standing: Diplomatic Protection 29
7.2.1 Applicant Arguments 29
7.2.2 Respondent Arguments 29
7.2.3 Suggested Questions 30
7.3 Freedom of Speech: Art 19 of the ICCPR 30
7.3.1 Applicant Arguments 30
7.3.2 Respondent Arguments 33
7.3.3 Suggested Questions 34
8. QP4: Legality of Applicant's Botnet Takedown Order 35
8.1 Introduction 35
8.2 Clean Hands Doctrine 36
8.2.1 Applicant Arguments 36
8.2.2 Respondent Arguments 36
8.3 Budapest Convention 37
8.4 Customary International Law 40
8.4.1 Applicant Arguments 40
8.4.2 Respondent Arguments 41
8.4.3 Suggested Questions 42
8.5 Circumstances Precluding Wrongfulness 44
8.5.1 Applicant Arguments 44
8.5.2 Respondent Arguments 44

2. PURPOSE OF THE BENCH MEMORANDUM

The Bench Memorandum provides judges with basic factual and legal information to evaluate the written memorials and oral pleadings of participating teams. It should be read in conjunction with the Jessup *Compromis* (including the Corrections & Clarifications).

The *Compromis* was designed to present the competitors with legal issues that have strengths and weaknesses on each side. Jessup teams should be able to construct logical arguments as both Applicant and Respondent. As a judge, your task is to evaluate the quality of each team's analysis, knowledge of international law, and advocacy skills. Please make sure not to confuse this task with an evaluation of the merits of the case. Your own views of the merits of the case should not influence your assessment of the quality of the teams' presentations.

The Bench Memorandum is not meant to be an exhaustive treatise on the legal issues raised in the *Compromis*. In many instances, relevant case law and State practice is alluded to, but is not discussed in depth. The State practice and legal authorities cited herein are illustrative and are not intended to be a comprehensive review of all relevant sources of law. Judges should expect participants to present arguments and to cite authorities that may not be discussed in this Memorandum.

As always, judges are encouraged to engage in their own independent research on the issues or to examine the suggested research materials given to students. These are available on our Competition Materials Page.

3. EXECUTIVE SUMMARY

The centerpiece of the *Compromis* concerns election interference, specifically, Respondent's financial contributions and cyber operations and the alleged dissemination of misinformation. The people of Sutha in Applicant wished to secede, and a referendum was scheduled for 1 March 2021. At the referendum, 52% voted for secession and 48% voted to remain. It was later discovered that:

- a 'botnet' which had infected over 30,000 devices over the 3 months leading up to the referendum was operated from premises in Respondent's territory;
- Respondent had made financial contributions to various Velan organisations in Sutha knowing that the money would be used in support of Suthan independence;
- Respondent had provided information on how to work around the identification verification process for the registration of social media accounts, and offered suggestions on how to create "masked" viral content to promote independence;
- Respondent formulated a plan for the initiation of a pro-independence propaganda campaign targeting Suthan citizens.

QP2 pertains to whether these acts, individually or collectively, amount to a breach of international law by Respondent.

To establish this breach, Applicant will rely on evidence which Respondent seeks to exclude. This evidence comprises (i) documents obtained in the search of the vehicle of the wife of Respondent's ambassador and (ii) the recording of a conciliation meeting between Applicant's and Respondent's representatives which all but confirmed the veracity of those documents.

The admissibility of these materials as evidence is the subject of **QP1**.

Prof. Liam Hunland is a citizen of Respondent but has been a legal permanent resident of Applicant since the 1980s. He is an advocate for Suthan autonomy and owns the third-largest (personal) Pano page in the region. Hunland established a non-profit organisation, Suthans Against Domination ("**SAD**"), which was later discovered to be operating the botnet from within Respondent's territory. Leading up to the referendum, Hunland continued criticising Applicant's government by, among other things, writing over 800 posts between November and December 2020, many of which were independently shown to be false. On 31 January 2021, Hunland staged an outdoor independence rally in violation of government Covid restrictions, and the resulting violence led to 225 injuries and three deaths. He later re-posted a picture of a police officer beating a woman at the rally which was, again, shown to be false.

Between January and February 2021, Pano (the largest social media platform in the region), implementing its content moderation policy, flagged about 63% of his posts and re-posts for inauthentic, false or malicious content. On 5 February, Applicant's Data Protection and Cybersecurity Agency ("**DPCA**"), acting under the Protect Antaran Cyberspace Act of 2017 ("**PACA**"), applied for and obtained (on 15 February 2021) an order from Applicant's court for the removal of Hunland's posts and the suspension of his accounts for a period of one year (later extended by court order). Hunland unsuccessfully applied to Applicant's courts for an injunction against the order, and to Zemin's courts to have the restrictions set aside (as Zemin was where Pano was incorporated).

QP3 presents the issue of whether Applicant's court order suspending Hunland's Pano account was consistent with international law. There is an antecedent question of whether Respondent may validly exercise diplomatic protection over him, because although Hunland is a citizen of Respondent, he has lived in Applicant since the 1980s and is a permanent resident there.

One week before the referendum, Applicant's DPCA sought and obtained a court order for the takedown of what was termed the "Lunar Botnet." The takedown, Operation Moonstroke, affected all of the hacked devices. It is undisputed that about 20,000 of those devices were situated in Applicant's territory, about 5,000 in Respondent's territory, and the rest in other locations.

QP4 asks whether Operation Moonstroke was in violation of international law, given that it affected devices in Respondent's territory without Respondent's consent. Both States are parties to the Budapest Convention.

In the sections below each QP is addressed in turn.

4. PRELIMINARY MATTERS

4.1 Jurisdiction

The basis of the Court's jurisdiction in this case is Article 36(1) of the ICJ Statute (i.e. by way of Special Agreement). Accordingly, the text of the *Compromis* should be read as a carefully negotiated agreement that was a result of extensive negotiation, and the jurisdiction of the Court will not likely be contested by either side.

4.2 Claims and Counterclaims

The *Compromis* contains two claims by Applicant (QPs 1 and 2) and two counterclaims by Respondent (QPs 3 and 4). Applicant's claims relate to the admissibility of evidence and the election interference while Respondent's counterclaims concern the suspension of Hunland's Pano account and the botnet takedown order.

With respect to counterclaims, Article 80 of the ICJ's Rules of Court provides: "The Court may entertain a counter-claim only if it comes within the jurisdiction of the Court and is directly connected with the subject-matter of the claim of the other party." That the counterclaims come within the Court's jurisdiction is not in dispute. And QPs 3 and 4 are "directly connected" with the subject-matter of QPs 1 and 2. So the jurisdiction of the Court to hear the counterclaims is also not likely to be in dispute.

4.2.1 Suggested Questions

Basic Questions	1. What are the four bases of the Court's jurisdiction generally? 2. What is the difference between a claim and a counterclaim?
Advanced Question	3. What are the requirements for the Court to entertain a counterclaim?

5. QP1: ADMISSIBILITY OF EVIDENCE

5.1 Introduction

This QP concerns the admissibility of: (1) documents obtained from Ms. Walters's briefcase and (2) the recording/transcript of an ad-hoc conciliation meeting between the Attorneys General of Antara and Ravaria.

The Relevant Facts for QP1

- Antaran police officers arrested Ms. Emma Walters (wife of the Ravarian Ambassador to Antara) after she killed a pedestrian while driving drunk. They seized an unmarked briefcase from her car, where they found her diplomatic passport and licence (¶35). They placed her passport in the pocket of her jacket (*Clarifications*, ¶4).
- She was brought back to the station and delivered to the duty sergeant. The arresting officers did not mention that Ms. Walters was connected to a foreign embassy (¶36) and her passport was no longer in the briefcase (*Clarifications*, ¶4).
- The duty sergeant opened the briefcase, and discovered documents revealing that: (¶37(a)-(d)):
    - Ravaria had channelled €25 million to SAD and SIP through its Embassy;
    - Ravaria had provided the Ambassador detailed instructions on how to conduct a misinformation campaign; and
    - SAD was operating a botnet from a server within its headquarters to "guide the hearts and minds of voters towards secession."
- Antara returned the documents to the Ravarian Embassy but made copies of them for "reasons of national security" (¶38).
- An Antaran criminal investigation later revealed that SAD had controlled the botnet from its servers. It also concluded that the funding by the Ravarian Embassy did not violate domestic campaign finance laws (¶39).
- The Attorneys General of Antara and Ravaria attended an ad-hoc conciliation meeting to resolve the dispute. During the meeting, the Attorney General of Ravaria conceded that he did not deny "that the papers say what you have reported" (¶44).
- Art. 2(b) of the Special Agreement provides that:

> *any reference in this Special Agreement to certain documents or recordings obtained and disclosed without the consent of Respondent is without prejudice to Respondent's position that these documents should not be accepted as evidence before the Court.*

Relevant Sub-Issues for QP1

- Were the documents obtained in breach of the Vienna Convention on Diplomatic Relations ("**VCDR**")?
- Should illegally obtained evidence be excluded?
- Should evidence from settlement negotiations be excluded?

5.2 Were the Documents Obtained in Breach of the VCDR?

Applicant may argue that the documents were not obtained in breach of the VCDR. If that argument prevails, the issue of their exclusion will fall away: there would be no basis for such a ruling. Some Applicant teams may choose to strategically concede that the documents were obtained illegally and to focus instead solely on the issue of their exclusion.

The relevant articles of the VCDR are Arts 24, 27(2), 29, and 37(1):[1]

> *Article 24*
> *The archives and documents of the mission shall be inviolable at any time and wherever they may be.*
>
> *Article 27(2)*
> *The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions.*
>
> *Article 29*
> *The person of a diplomatic agent shall be inviolable. He shall not be liable to any form of arrest or detention. The receiving State shall treat him with due respect and shall take all appropriate steps to prevent any attack on his person, freedom or dignity.*
>
> *Article 37(1)*
> *The members of the family of a diplomatic agent forming part of his household shall, if they are not nationals of the receiving State, enjoy the privileges and immunities specified in articles 29 to 36.*

Art 27(3) is not engaged as the briefcase did not have the markings required under Art 27(4), and hence was not a diplomatic bag.

5.2.1 Applicant Arguments

Applicant may argue, under Art. 24, that diplomatic documents are protected only if they are under the actual control of a member of the mission. This interpretation is supported by the recent UK Supreme Court decision in *Bancoult (No. 3)*,[2] in relation to documents obtained from Wikileaks:

> *The relevant point for present purposes is that because the designation of a document as that of the mission depends on control, its origin and content is in itself irrelevant. Thus the archives and documents of a mission may include original or copy documents which emanate from some other organ of the sending state or from a third party, in which case so far as they are under the control of the mission's personnel they will enjoy the same protection as the mission's internally generated documents. Correspondingly, copy documents or originals emanating from the mission may be found in the archives of another organ of the state (say, its foreign ministry) where they will not enjoy the*

---

[1] Vienna Convention on Diplomatic Relations (1964) 500 UNTS 95. Both Antara and Ravaria are parties to the VCDR (¶46).

[2] *R. (on the application of Bancoult No 3) v Secretary of State for Foreign and Commonwealth Affairs* [2018] UKSC 3, para. 68.

protection of article 24.

The Court relied on the House of Lords' decision in *Shearson Lehman Brothers Inc v Maclaine Watson & Co Ltd* [1988] 1 WLR 16, 29. Further, as Eileen Denza notes in *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations* (Fourth Ed., Oxford University Press 2016) ("**Diplomatic Law**") at p.162:

> *It would follow that correspondence to or documents supplied to a third party not being a member of the diplomatic mission or in any other capacity an employee of the sending State would normally become the property of the recipient and so would no longer form part of the archives and documents of the mission.*

Diplomatic Law, at p.189, also notes that "*[a]s regards use of correspondence as evidence, Article 27.2 may be regarded as duplicating the protection under Article 24 of the Convention which gives inviolability to the archives and documents of the mission 'wherever they may be'.*" Accordingly, what is true of "archives and documents" under Art 24 should apply in a similar fashion to "correspondence" under Art 27.

5.2.2 Respondent Arguments

Respondent may argue that, having regard to the object and purpose of the VCDR, as well as the ordinary meaning of the words "*at any time and wherever they may be*" in Art 24, diplomatic documents are always inviolable. This interpretation is supported by the drafting history of the VCDR. As noted in *Diplomatic Law* at p.158, the International Law Commission added the words "wherever they may be" to the draft treaty to make it "*clear beyond argument that archives not on the premises of the mission and not in the custody of a member of the mission are entitled to inviolability*".[3]

Respondent may also rely on the Partial Award of the Eritrea Ethiopia Claims Commission of 19 December 2005.[4] There, Eritrean customs officials intercepted and retained a diplomatic bag (not correctly labelled as such) containing blank passports. The Commission found that Eritrea breached Art 24 of the VCDR by retaining the bag after its "*official character became apparent*".

5.2.3 Suggested Questions

Basic Questions	1. How should Art 24/27(2) VCDR be interpreted?
Advanced Questions	1. (For Applicant) How does your narrow reading of Art 24 accord with the object and purpose of the VCDR? 2. What are the appropriate remedies for a breach of the VCDR?

[3] Recourse may be had to the preparatory work of the treaty to "*confirm*" its meaning pursuant to Art 32 VCLT.
[4] *Diplomatic Claim—Ethiopia's Claim 8 (Eritrea/Ethiopia)* [2005] PCA Case No. 2001-02, para 44.

5.3 Exclusion of the Documents Obtained from the Briefcase

Beyond procedural requirements, both the ICJ Statute and the Rules of Court are deliberately broad regarding the issue of the admissibility of evidence. Art 48 of the Statute provides:

> *The Court shall make orders for the conduct of the case, shall decide the form and time in which each party must conclude its arguments, and make all arrangements connected with the taking of evidence.*

Art 62(1) of the Rules of Court states:

> *The Court may at any time call upon the parties to produce such evidence or to give such explanations as the Court may consider to be necessary for the elucidation of any aspect of the matters in issue, or may itself seek other information for this purpose.*

Nothing in the Statute, Rules, or Practice Directions expressly addresses admissibility, let alone admissibility of illegally obtained evidence.

Accordingly, this QP has been **deliberately designed for Respondent to have to find/craft a rule** by which the Court could exclude such evidence.

This QP is particularly important for Applicant, as the material in dispute is critical to its position on the subsequent QPs. Judges may wish to ask Applicant about the consequences for the remainder of the case if the Court rejects its argument and decides to exclude the proffered evidence.

5.3.1 Applicant Arguments

Applicant will argue that there is no exclusionary rule in international law barring the admissibility of material obtained illegally. For example, President Spender in *South West Africa* observed:[5]

> *The evidence will remain on the record; the Court is quite able to evaluate evidence, and if there is no value in the evidence, then there will be no value given to this part of the evidence...This Court is not bound by the strict rules of evidence applicable in municipal courts and if the evidence established by the witness does not sufficiently convey that the evidence is reliable in point of fact, then the Court, of course, deals with it accordingly when it comes to its deliberation.*

The ICJ's evidentiary regime has been described as based on the "*principle of free admissibility*".[6]

Applicant may also rely on *Corfu Channel.* In that case, the UK conducted a minesweeping operation in Albania's territorial waters after mines damaged two of its vessels, obtaining physical evidence that it claimed supported its case before the Court. It argued that the operation was justified and was not an illegal infringement of Albanian sovereignty.[7] The Court was not persuaded; it held that the operation violated

---

5 *South West Africa*, Second Phase, [1966] Pleadings-X, 122; XI, 460.

6 Chen, Siyuan, '*Re-assessing the evidentiary regime of the International Court of Justice: A case for codifying its discretion to exclude evidence*' (2015) *International Commentary on Evidence* 13(1) 1-40 Research Collection School Of Law ("**Chen (2015)**").

7 *Corfu Channel (UK/Albania)* [1949] (Merits) ICJ Rep. 4, p.34.

international law, and rejected the right to 'discovery by intervention'. As observed by S Mansour Fallah, however:[8]

> *The Court did not discuss the issue of admissibility of the evidence gained through the territorial intrusion at all and ultimately even used some of the evidence obtained in the unlawful minesweeping mission to corroborate a violation of international law by Albania.*

Accordingly, Applicant may argue that illegally obtained evidence should not be excluded. Applicant may contend that Respondent's argument, that to allow such evidence would condone a breach of international law, is inconsistent with the outcome in *Corfu Channel*.

Applicant may also submit that there is no rule, custom or general principle of international law that bars the admission of illegally obtained evidence.

A general principle of law must be "widely accepted" in national legal systems and capable of transposition into international law. A study of the evidentiary rules relating to illegally obtained evidence in civil proceedings in 27 jurisdictions across all five UN Regional Groups in 2015 showed that positions on the admission of illegally obtained evidence ranged from considering them to be generally admissible to excluding them in all circumstances, with option in between.[9]

Applicant may provide specific examples to demonstrate that the exclusion of illegally obtained evidence is not "widely accepted" in national jurisdictions. Applicant may also argue that the principle is not sufficiently established across the various types of legal systems. In its *Lubanga* decision, the ICC explained, regarding the preparation of witnesses before their testimony:[10]

> *Although this practice is accepted to an extent in two legal systems, both of which are founded upon common law traditions, this does not provide a sufficient basis for any conclusion that a general principle based on established practice of national legal systems exists. The Trial Chamber notes that the prosecution's submissions with regard to national jurisprudence did not include any citations from the Romano-Germanic legal system.*

Applicant may also argue that international tribunals that have excluded illegally obtained evidence did so in accordance with their particular rules of procedure. For example, Art 69(7) of the Rome Statute provides that evidence obtained by a breach of the treaty or internationally recognised human rights shall not be admissible if the violation casts substantial doubt on the reliability of the evidence or if its admission would be antithetical to the integrity of the proceedings. Rule 95 of the Rules of Procedure of the ICTY and ICTR is to the same effect. Similarly, in the *Methanex* Award, the tribunal relied on Art 15(1) of the UNCITRAL Rules on procedural fairness to exclude unlawfully obtained evidence.[11] Applicant can argue that the Court should not reach the same result in the absence of a specific procedural rule.

---

[8] Mansour Fallah, Sara, '*The Admissibility of Unlawfully Obtained Evidence before International Courts and Tribunals*' (2020) The Law and Practice of International Courts and Tribunals 19, pp.147–176.

[9] Chen (2015) at Chapter 4 – Deriving a General Principle from National Laws? – A Comparative Study of National Civil Procedure.

[10] *Prosecutor v. Thomas Lubanga Dyilo*, Decision Regarding the Practices Used to Prepare and Familiarise Witnesses for Giving Testimony at Trial (1 December 2007) ICC-01/04-01/06-1049, p. 41..

[11] *Methanex v USA (Final Award, 3 August 2005)* Part II, Chapter I, para 54.

Alternatively, even if the Court were to find that illegally obtained material should generally be excluded, Applicant may argue that this case deserves an exception. Applicant may propose a "balancing exercise," considering the egregiousness of the breach against the relevance and reliability of the evidence sought to be excluded. For example, the ICJ in *Armed Activities* observed that it would:[12]

> *identify the documents relied on and make its own clear assessment of their weight, reliability and value. In accordance with its prior practice, the Court will explain what items it should eliminate from further consideration.*

Given its potential value, it will be difficult for Respondent to argue that the evidence is not relevant or probative. The documents directly show Respondent's involvement in the activities that Applicant alleges in QP2 constituted illegal election interference..

5.3.2 Respondent Arguments

Respondent may argue that there is a general rule of international law under which material obtained in breach of international law should not be admitted into evidence.

Respondent may rely on *Corfu Channel*, arguing that while the Court did not approve of the UK's acts,[13] it ultimately allowed the evidence to be considered only because Albania had not sought its exclusion. This was also the interpretation of Judge Tomka, who wrote that "*unlawfully obtained proof may obviously be excluded*" based on the *Corfu Channel* case.[14] His views are relevant under Art 38(1)(d) ICJ Statute.

Respondent may also attempt to crystallise a general principle of law (under Article 38(1)(c) of the Statute) to the effect that illegally obtained evidence is inadmissible. Stronger Respondent teams will attempt to develop an exclusionary rule under the broader umbrellas of "good faith" and "procedural fairness". This was the position taken by the arbitral tribunal in *EDF v Romania* (Procedural Order No. 3) in excluding illegally recorded conversations from evidence.[15]

Respondent can also point to the Court's decision in *Timor-Leste v. Australia*.[16] The case concerned the seizure by Australia of certain documents belonging to Timor-Leste's legal counsel. Timor-Leste alleged that these were correspondence between its government and legal advisors relating to a pending arbitration between the parties and requested the Court to order their return. In its provisional measures judgment, the Court held that:[17]

> *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*

---

[12] See *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)*, [2005] ICJ Rep 168 at para 298.

[13] At p.35.

[14] H.E. Peter Tomka and Vincent-Joël Proulx, "The Evidentiary Practice of the World Court" in Juan Carlos Sainz-Borgo et al. (eds), Liber Amicorum in Honour of a Modern Renaissance Man: His Excellency Gudmundur Eiríksson (University for Peace Press 2016), p.369.

[15] *EDF v Romania (Procedural Order No.3)* [2008] ICSID Case No. ARB/05/13, para. 38..

[16] *Questions relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), Provisional Measures, Order of 3 March 2014* [2014] ICJ Rep.147 ("**Timor-Leste**").

[17] *Timor-Leste*, paras 28-30.

well as to the protection of confidentiality of any documents and data prepared by counsel to advise that State in such a context

...

The Court considers that these measures by their nature are intended to protect Timor-Leste's claimed rights to conduct, without interference by Australia, arbitral proceedings and future negotiations, and to communicate freely with its legal advisers, counsel and lawyers to that end. The Court thus concludes that a link exists between Timor-Leste's claimed rights and the provisional measures sought.

While this decision did not relate to the exclusion of such evidence from ongoing litigation, some Respondent teams may attempt to urge extension of the Court's order by analogy.

Stronger Respondent teams should also be able to weave policy objectives (*e.g.*, that admission of the evidence would mean that the Court would essentially condone illegality) into their arguments. Respondent may contend that such an exclusionary rule would be consistent with the general principle of law that no party should be allowed to benefit from its own wrongdoing.[18]

5.3.3 Suggested Questions

Basic Questions	1. Does the ICJ have any rules governing the admissibility of evidence? 2. What is a general principle of international law? How can it be established? 3. Have there been any cases in which this Court has excluded evidence on the basis that it was illegally obtained? 4. Have there been any decisions of international tribunals which have excluded illegally obtained evidence?
Advanced Questions	1. (For Applicant) Would the admission of these documents encourage future parties to engage in illegal activities? Should the Court condone such conduct? 2. (For Respondent) How does this exclusionary rule accord with the Court's approach to dealing with documentary evidence in cases such as *Whaling*, *Armed Activities* and *Pulp Mills*? 3. Are the decisions in *Corfu Channel* and *Tehran Hostages* applicable/distinguishable? Why? 4. Have any courts/tribunals dealt considered what constitutes a general principle of international law in the context of evidentiary questions? 5. What weight (if any) should this Court give to the Draft Conclusions of the ILC on General Principles of Law? 6. (For Applicant) Even if the evidence is admissible, should the court give it any weight? 7. (For Respondent) Is there any difference between finding the evidence inadmissible and admitting it but assigning it little to no weight? What prejudice would Ravaria suffer?

[18] Bin Cheng, *General Principles of Law as applied by International Courts and Tribunals* (Steven & Sons 1953), p 149

5.4 Admissibility of the Conciliation Transcript/Recording

In the 1927 PCIJ *Factory at Chorzow* decision, the Court noted that it:[19]

> *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*

The status of this as a customary rule has since been reaffirmed in the ICJ's decisions in *Land, Island and Maritime Frontier Dispute*[20] and *Maritime Delimitation (Qatar/Bahrain)*[21]. However, in *Frontier Dispute*, the Court further clarified the rule:

> *This observation however refers to the common and laudable practice - which, indeed, is of the essence of negotiations - whereby the parties to a dispute, having each advanced their contentions in principle, which thus define the extent of the dispute, proceed to venture suggestions for mutual concessions, within the extent so defined, with a view to reaching an agreed settlement. If no agreement is reached, neither party can be held to such suggested concessions.*

Applicant seeks to have the official transcript of the conciliation meeting (¶44) accepted as evidence because it will support the position that the documents from Ms. Walters's briefcase are reliable. There is an argument to be made that the statements by Respondent's AG amount to such a concession. Good teams should carefully discuss and reference the precise language used.

5.4.1 Applicant Arguments

Applicant will argue that the transcript is not a "suggestion for mutual concession … with a view to reaching an agreed settlement," as required by *Land, Island and Maritime Frontier Dispute*. While the Ravarian Attorney-General stated that he was "*not denying that the papers say what you have reported*", this does not appear to concede Applicant's position in relation to any of the substantive matters in dispute. Applicant may also argue that the statements made in the transcript appear to evince no more than the "*shared view of the parties as to the basis and extent of the dispute*". In *Land, Island and Maritime Frontier Dispute*, the Court held that it could not take into account the negotiating concessions which might have been made as to their "positions", but could consider matters that the parties agreed were not in dispute. Applicant could argue that the statements made by the Attorneys General show that they shared a view that the contents of the documents from the briefcase were true.

Alternatively, Applicant may argue that there was an agreement reached as to the diplomatic incident involving Ms. Walters. The parties signed an agreement whereby the Ravarian government would pay an undisclosed sum to Mr. Francis's family while Antara agreed to apologise for the arrest of Ms. Walters.[22] Accordingly, a complete agreement was reached in relation to the diplomatic incident (in which context the statement was made).

---

[19] *Case Concerning the Factory at Chorzow* (1927) PCIJ Series A, No 9.
[20] *Land, Island, and Maritime Frontier Dispute (El Salvador/Honduras)* [1992] ICJ Rep. 351, para 73.
[21] *Maritime Delimitation and Territorial Questions between Qatar and Bahrain, Merits, Judgment, 1.C.J. Reports 2001,* p. 40
[22] ¶43.

Applicant teams may also argue that the statements of the Ravarian Attorney General were merely a reiteration of those made by the Minister for External Affairs in May 2021 (at ¶41) and should therefore not fall within the rule in *Factory at Chorzow* at all.

5.4.2 Respondent Arguments

Respondent is likely to assert that the statement falls into the scope of "*declarations, admissions or proposals*" in *Factory at Chorzow*. The statement by the Ravarian Attorney General in relation to the briefcase documents goes to the heart of the dispute over the issues of election interference and botnet takedowns, which were not the subject of any agreement between Antara and Ravaria. In fact, the preamble to the Special Agreement expressly notes "*that the Parties have been unable to resolve these differences by direct negotiations.*"

5.4.3 Suggested Questions

Advanced Questions	1. (For Applicant) If this Court excludes the evidence, would that not encourage parties to refrain from open and candid settlement negotiations? 2. (For Applicant) If we decline to admit the evidence, what impact will that have on the /reliability of the briefcase documents? 3. (For Applicant) What is the relevance, if any, of the decision of this Court in the *Frontier Disputes* case? 4. (For Applicant) How can there be a "complete agreement" if the preamble to the Special Agreement expressly notes that the parties have been unable to resolve the dispute by direct negotiation? 5. (For Respondent) If the Attorneys General did not agree that the transcript could not be used for any reason, why should the Court impute that intention to them? 6. (For Respondent) Does the transcript not simply record the "shared views" of the parties per *Land, Island and Maritime Frontier Dispute*?

6. QP2: ELECTION INTERFERENCE

6.1 Introduction

This QP pertains to the legality of Respondent's financial contributions and cyber operations in connection with the Suthan referendum. The rest of this section proceeds on the basis that the evidence under QP1 has been admitted.

The Relevant Facts for QP2

- Sutha is a province of Antara and is home to the Kuvil Shrine, an important landmark in the Velan religion (¶1-2). 47% of Suthans and 85% of Ravarians identify as Velan (¶5).
- The 1962 Treaty of Singapore provides that the Suthan Legislative Council and the Antaran Parliament could authorise a referendum in Sutha and that the two states would respect the result of the referendum. This was codified in the Antaran Constitution (¶6).
- The pro-independence Suthan Independence Party ("SIP") had 10-20% of the votes in local and national elections between 1963 and 2008. This share increased, so that SIP had 55 out of 130 seats in the Suthan Legislative Council and 41 of 250 in the Antaran Parliament by 2016 (¶7, 14). In June 2020, Hunland founded a non-profit called Suthans Against Domination ("**SAD**") (¶16).
- In October 2020, the Antaran government agreed to hold the referendum, scheduling it for 1 March 2021 (¶21).
- With 67% turnout, the result of the vote was that 52% supported secession.
- The documents from Ms. Walters's briefcase later revealed that €25 million had been channeled to SAD and SIP, that the Ambassador had received emails from the Ravarian External Affairs Ministry on how to automate registration on Pano and "mask" content such that it would appear it had come from within Antara/Sutha, that SAD was operating a botnet from within its headquarters producing misinformation to urge voters to vote for secession and that the Ravarian government had detailed plans for a top-secret campaign to unite Sutha with Ravaria (¶37).
- On 7 May 2021, the Ravarian Foreign Minister acknowledged that Ravaria had exercised "*political influence*" in the referendum and had done so "*with pride*", stating that they would continue to engage in such practices (¶41).

Relevant Sub-Issues for QP2

The facts suggest two kinds of election interference: (1) the misinformation by SAD and (2) the funding of SAD and SIP by the Ravarian Embassy. For Respondent to be responsible for (1) SAD's campaign must be attributable to Ravaria.

6.2 Attribution of SAD's Misinformation Campaign

Whether the interference by SAD in the Suthan Referendum was attributable to Ravaria will require analysis of Arts 4 – 11 of the Articles on the Responsibility of States for Internationally Wrongful Acts ("**ARSIWA**").[23]

[23] Articles on Responsibility of States for Internationally Wrongful Acts (2001) UN Doc. A/56/10.

Articles 8 and **11** ARSIWA are the most relevant:

Article 8
Conduct directed or controlled by a State

The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

Article 11
Conduct acknowledged and adopted by a State as its own

Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own.

6.2.1 Applicant Arguments on Art 8 ARSIWA

Applicant may first suggest that the "control" within Art 8 means only "*overall control,*" as suggested by the ICTY in *Tadic*.[24] However, this was expressly rejected by the ICJ in *Bosnian Genocide*:[25]

Apart from these cases, a State's responsibility can be incurred for acts committed by persons or groups of persons — neither State organs nor to be equated with such organs — only if, assuming those acts to be internationally wrongful, they are attributable to it under the rule of customary international law reflected in Article 8 cited above (paragraph 398). This is so where an organ of the State gave the instructions or provided the direction pursuant to which the perpetrators of the wrongful act acted or where it exercised effective control over the action during which the wrong was committed. In this regard the "overall control" test is unsuitable, for it stretches too far, almost to breaking point, the connection which must exist between the conduct of a State's organs and its international responsibility.

Accordingly, the Court is unlikely to adopt the "*overall control*" test.

Applicant may therefore rely on the "*effective control*" test (as the term was used in *Nicaragua*.[26] As noted in *Bosnian Genocide* at para 400, there is no need to show that the entity carrying out the activity was in a relationship of complete dependence on the State:

First, in this context it is not necessary to show that the persons who performed the acts alleged to have violated international law were in general in a relationship of "complete dependence" on Respondent State; it has to be proved that they acted in accordance with that State's instructions or under its "effective control". It must however be shown that this "effective control" was exercised, or that the

---

[24] *The Prosecutor v. Duško Tadić* (1999) (Judgment of the Appeals Chamber) IT-94-1-A, para 145.

[25] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia & Herzegovina/Serbia & Montenegro)* 2007 ICJ Rep. 43 ("***Bosnian Genocide***") at paras 402-407.

[26] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua/United States of America)* [1986] ICJ Rep. 64, para 115.

> *State's instructions were given, in respect of each operation in which the alleged violations occurred, not generally in respect of the overall actions taken by the persons or groups of persons having committed the violations.*

Here, Respondent gave clear authorisation and approval for the botnet as part of its broader influence campaign (¶37). Significant funding was also given to SAD by the Ravarian government. While nothing in the Compromis suggests that Respondent provided specific instructions for the operation of the botnet, Applicant may argue that such instruction can be inferred from the circumstantial evidence within the *Compromis*. Applicant can point to the decision in *Corfu Channel*, where the Court permitted the United Kingdom "*liberal recourse to inferences of fact*" regarding Albania's knowledge of location of the mines in the Channel, as the evidence was within Albania's "*exclusive territorial control*".[27]The evidence of whether Ravaria gave direct instruction to SAD is similarly within Respondent's exclusive control.

6.2.2 Respondent Arguments on Art 8 ARSIWA

Respondent will argue that the overall control test is inapplicable. As discussed above, this is not controversial given the statements of the ICJ in *Bosnian Genocide*.

Respondent may also argue that it never had effective control over the acts of SAD.[28] For example, in *Nicaragua*, the Court observed:

> *All the forms of United States participation mentioned above, and even the general control by the respondent State over a force with a high degree of dependency on it, would not in themselves mean, without further evidence, that the United States directed or enforced the perpetration of the acts contrary to human rights and humanitarian law alleged by the applicant State. Such acts could well be committed by members of the contras without the control of the United States. For this conduct to give rise to legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed.*

Ravaria may claim an analogy to the acts of the contras, because any "control" exercised by Ravaria was no more than "general," regardless of how much SAD depended on it. However, the fact that Respondent did not have "effective control" over SAD, and in particular did not provide instructions for each specific operation (per *Bosnian Genocide* at para 400), would render Respondent not responsible for whatever SAD may have done.

6.2.3 Applicant Arguments on Art 11 ARSIWA

Applicant may rely on Art 11 ARSIWA to argue that Respondent acknowledged and adopted the conduct of SAD as its own. The ILC's Commentary on Art 11 refers to the decision in *Tehran Hostages*, where the

---

[27] *Corfu Channel*, p.18.
[28] *Nicaragua*, para 115.

Court distinguished the seizure of the United States embassy by militants from the Iranian State's approval and maintenance of the situation:[29]

> *The policy thus announced by the Ayatollah Khomeini, of maintaining the occupation of the Embassy and the detention of its inmates as hostages for the purpose of exerting pressure on the United States Government was complied with by other Iranian authorities and endorsed by them repeatedly in statements made in various contexts. The result of that policy was fundamentally to transform the legal nature of the situation created by the occupation of the Embassy and the detention of its diplomatic and consular staff as hostages. The approval given to these facts by the Ayatollah Khomeini and other organs of the Iranian State, and the decision to perpetuate them, translated continuing occupation of the Embassy and detention of the hostages into acts of that State.*

The Commentary also cites the Eichmann Incident as an example of State practice as to acknowledgment and adoption, particularly where there were "*doubts about whether certain conduct falls within article 8*":[30]

> *Security Council resolution 138 (1960) of 23 June 1960 implied a finding that the Israeli Government was at least aware of, and consented to, the successful plan to capture Eichmann in Argentina. It may be that Eichmann's captors were "in fact acting on the instructions of, or under the direction or control of" Israel, in which case their conduct was more properly attributed to the State under article 8. But where there are doubts about whether certain conduct falls within article 8, these may be resolved by the subsequent adoption of the conduct in question by the State.*

Here, Respondent's Minister of External Affairs stated on 7 May 2021 that Respondent "*makes no apology for its investment of resources in the promotion of Velan ideals globally.*" He said that *"We do this with pride*" and would "*continue to engage*" in such practices (¶41). Further, Respondent has not taken any action against SAD to prevent the further spread of misinformation. The botnet was taken down by Antara only during "Operation Moonstroke," suggesting that Respondent had allowed the election involvement to continue, as had the Iranian government in *Tehran Hostages* and the Israeli government during the Eichmann Incident.

6.2.4 Respondent Arguments on Art 11 ARSIWA

Respondent will argue that there is a distinction between statements of approval and assumption of responsibility. As noted in the ILC's Commentary to ARSIWA Art 11:[31]

> *In international controversies, States often take positions which amount to "approval" or "endorsement" of conduct in some general sense but do not involve any assumption of responsibility. The language of "adoption", on the other hand, carries with it the idea that the conduct is acknowledged by the State as, in effect, its own conduct. Indeed, provided the State's intention to accept responsibility for otherwise non-attributable conduct is clearly indicated, article 11 may cover cases where a State has accepted responsibility for conduct of which it did not approve, which it had sought to prevent and which it deeply regretted. However such acceptance may be phrased in the particular case, the term*

---

[29] *United States Diplomatic and Consular Staff in Tehran (USA/Iran)* [1980] (Merits) ICJ Rep. 3, para 74.

[30] Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries (2001) UN Doc. A/56/10 ("**ARSIWA Commentary**") at p.53.

[31] ARSIWA Commentary, Art 11, para 6 at p.53.

> *"acknowledges and adopts" in article 11 makes it clear that what is required is something more than a general acknowledgement of a factual situation, but rather that the State identifies the conduct in question and makes it its own.*

Respondent will likely argue that the statements by the Ravarian Minister for External Affairs amount to a general approval of SAD's position in the referendum rather than an assumption of responsibility for specific acts. An approval or endorsement in "some general sense" is insufficient to establish attribution under Art 11.

Further, Respondent will assert that it had no opportunity to address any allegations regarding improper cyber-operations as Applicant launched Operation Moonstroke to disable the botnet before it was notified.

6.2.5 Suggested Questions

Basic Questions	1. What are the requirements for an internationally wrongful act? 2. What is the status of the Articles on State Responsibility? Can this Court rely on them, and if so, why?
Advanced Questions	1. (For Applicant) How can "effective control" be established in the absence of specific instructions from Respondent state on the operation of the botnet? 2. (For Respondent) Can an adverse inference be drawn against Respondent for failing to produce evidence within its exclusive territorial control? 3. (For Applicant) Did Respondent perpetuate the conduct of SAD given that Operation Moonstroke disabled the botnet before it could take any action?

6.3 Legality of SAD's Misinformation Campaign

One issue here is whether the misinformation campaign violated the principle of non-intervention under the UN Charter and customary international law. In *Nicaragua*, the Court explained:[32]

> *In this respect it notes that, in view of the generally accepted formulations, the principle forbids all States or groups of States to intervene directly or indirectly in internal or external affairs of other States. A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy. Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.*

Accordingly, there are two requirements for a breach of the principle of non-intervention: the act in question must affect another State's internal affairs, and it must be coercive, effectively depriving the target State of the ability to control or govern affairs which a State would otherwise be able to decide freely.

[32] *Nicaragua*, para 205.

This has been cited in Rule 66.1 of the Tallinn Manual 2.0 as applying to cyberspace: *A State may not intervene, including by cyber means, in the internal or external affairs of another State.*

Further, the UN Group of Governmental Experts in its Report dated 22 July 2015 on the "Developments in the Field of Information and Telecommunications in the Context of Internal Security"[33] identified non-intervention as one of the principles of international law which apply in the context of "*information and communications technologies*".[34]

6.3.1 Applicant Arguments on Non-Intervention

First, Applicant teams must demonstrate that the secession referendum was a matter exclusively within its own internal affairs (or its *domaine réservé*).

Applicants must also show that acts attributable to Respondent amounted to coercion. There is no clear agreement on when interference in an election is coercive, but there are clear-cut cases of what would and would not be unlawful. Coercion that would be illegal includes acts which take away from a State's ability to conduct its elections, such as disabling election machinery or tampering with the vote count.[35] But according to the Tallinn Manual 2.0, "*coercion must be distinguished from persuasion, criticism, public diplomacy, propaganda ... unlike coercion, such activities merely involve either influencing (as distinct from factually compelling) the voluntary actions of the target State, or seek no action on the part of the target State at all*".[36]

The present situation falls somewhere between those two extremes.

Applicant may attempt to draw a parallel with the ICJ's decision in *Nicaragua*:[37]

> *in international law, if one State, with a view to the coercion of another State, supports and assists armed bands in that State, that amounts to an intervention by the one State in the internal affairs of the other, whether or not the political objective of the State giving such support and assistance is equally far-reaching … the support given by the United States, up until the end of September 1984, to the military and paramilitary activities of the contras in Nicaragua, by financial support, training, supply of weapons, intelligence and logistic support, constitutes a clear breach of the principle of non-intervention*

Applicant will argue that Respondent had similarly given financial support, training (such as information as to how to get past Pano's account verification security process), and intelligence (information as to what types of posts would likely go viral), and it also approved of and supported SAD's botnet (¶41). Applicant

---

[33] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2015) UN Doc. A/70/174 ("**GGE Report**")

[34] GGE Report at paras 26 and 28(a).

[35] As analysed by Professor Michael Schmitt in "*Foreign Cyber Interference in Elections*" (2021) 97 Int'l L Stud 739, available online at https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2969&context=ils ("***Foreign Cyber Interference***") at p.747.

[36] Rule 66, para 21 rather than any breach of international law.

[37] *Nicaragua*, paras 241 to 242.

can also point to the fact that Respondent knew that Antara was bound by obligations within its constitution and by the Treaty of Singapore to respect the outcome of the referendum (¶6).

Coercion, of course, need not involve force or the threat of force. The parties may be expected to argue whether the religious and/or cultural appeals made by SIP and SAD – assuming that they are attributable to Respondent – amounted to coercion. This question may turn on whether Antaran voters in the referendum were in some manner deprived of their ability to make a free choice, or whether they felt constrained by the messages that they were receiving.

6.3.2 Applicant Arguments on Sovereignty

Applicant will argue that Respondent's acts constituted a breach of the obligation to respect its sovereignty under Art 2(1) of the UN Charter and customary international law, which is independent of the principle of non-intervention, enshrined in Art 2(4) of the Charter, prohibiting the threat or use of force against the "territorial integrity or political independence" of any State.

Applicant needs to establish that cyber activities can, in principle, implicate the need to respect that obligation. To do this, Applicant will refer to statements made by a number of States including Finland, France, the Netherlands, Germany, Iran, the Czech Republic, Austria and Switzerland that cyber activities can breach States' sovereignty even without any form of prohibited intervention.[38]

It should be noted that the UK rejects this position. Former Attorney-General Jeremy Wright said in a 2018 speech, "Cyber and International Law in the 21st Century":[39]

> *Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law.*

It appears that the UK is the only State which has publicly espoused this view. The practice of other States is likely sufficient to demonstrate widespread and virtually uniform state practice. If pushed, Applicant is likely to argue that the UK may be characterised as a persistent objector.

The concept of 'sovereignty' comprises 'territorial integrity' and activities which, without regard to territory, are 'inherently governmental functions':

- **Island of Palmas Arbitration**: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State"[40]

---

[38] See the practice of such States summarised in *Foreign Cyber Interference* at pp.750-751.

[39] See https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century

[40] At p.838.

- **Tallinn Manual 2.0**: an alleged breach of sovereignty may be assessed on two levels: "the degree of infringement upon the target State's territorial integrity" and "whether there has been an interference with or usurpation of inherently governmental functions".[41]

Applicant will likely focus its arguments on threats to political independence and inherently governmental functions as more relevant to the present facts. To demonstrate a breach of the obligation to respect its sovereignty, it need not show coercion or any physical or functional effects – it will contend that the mere fact of interference suffices.[42] Applicant will argue that the disinformation campaign constituted an interference into matters which were exclusively its own governmental functions.

6.3.3 Respondent Arguments on Non-Intervention

First, Respondent will argue that there is an antecedent issue of whether the acts that Applicant suggests should be attributed to it can be considered cumulatively. Respondent will point to the *Nicaragua* decision, where the Court approached the acts of funding, training, supplying weapons and intelligence, and others as *discrete* and analysed their legality individually. In no decision has this Court analysed alleged acts of coercion collectively.

Second, Respondent will argue that its acts at most amounted to attempts to *influence* rather than to *coerce* any acts of Applicant or its citizens, which is consistent with State practice. For example:

- The creation of inauthentic social media accounts during the 2016 US elections. Even though the Russian Internet Research Agency created thousands of social media accounts spreading misinformation in the United States, the Obama administration issued a carefully-worded statement referring to "*Russia's efforts to undermine established international norms of behavior, and interfere with democratic governance*". It did not suggest that they constituted a breach of international law.[43]
- In relation to the 2020 elections the United States again did not take the position that foreign election interference violated international law. The National Intelligence Council report, "*Foreign Threats to the 2020 US Federal Elections*", identified "*social media accounts covertly operated by Russia and Iran*", and determined that the Lakhta Internet Research agency (successor to the Internet Research Agency) had "*used social media personas, news websites, and US persons to deliver tailored content to subsets of the US population*". The United States still did not formally allege that the campaign was in violation of international law.

Regarding funding, Respondent may also point to States' financial support in foreign elections, including US provision of about $2.6 million for Chilean political candidate Eduardo Frei Montalva and Soviet government funding to the Communist Party of Chile of about $50,000 to $400,000 annually. Teams may provide additional examples of State practice to bolster this argument.

---

[41] Rule 4, paragraph 10.

[42] *Foreign Cyber Interference* p.753.

[43] See, for example: https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity.

Respondent may rely on the minority of the International Group of Experts which took the view that to constitute a threat to state sovereignty, a cyberactivity must "*directly cause the effect*".[44] Some statements issued by States arguably support this. For example, Australia has asserted that "*the use by a hostile State of cyber activities to manipulate the results of an election in another State ... would constitute a violation of the principle of non-intervention*".[45]

6.3.4 Respondent Arguments on Sovereignty

Respondent will argue that Applicant would impose liability in almost every instance where one State supports a particular political group or cause in another State's election. State practice does not support this.

Respondent may also rely on Professor Schmitt's observation that it is an open question whether "*cyber activities involving information or disinformation that [do] not affect how the election is carried out ever violate sovereignty*".[46]

Again, the arguments of good Applicant and Respondent teams are expected to be based in State practice rather than technical legal principles.

6.3.5 A Note on the Principle of Self-Determination

The principle of self-determination provides, at a minimum, that peoples must be able to determine their own political status and freely pursue their own economic, social, and cultural development (Art 1(1) ICCPR). The importance of this principle is enshrined in the UN Charter: Art 1(2) describes one of the purposes of the UN as to develop friendly relations among nations "*based on respect for the principle of equal rights and self-determination of peoples*". Art 55(1) provides that the UN shall promote international economic and social cooperation "*[w]ith a view to the creation of conditions of stability and well-being which are necessary for peaceful and friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples*".

The challenge that teams seeking to employ this well-established principle will face is *how* to use it to show that international law was or was not breached.

Applicant may argue that Respondent violated the principle of self-determination in depriving the Suthan people of the right to determine their own political future or to freely pursue the development of their own culture as expressed through the election.

Respondent may argue that the principle of self-determination cannot be independently breached but rather finds expression in a number of other different doctrines under international law, *e.g.* the human rights provisions of the ICCPR and such principles as the obligation of non-interference. This is consistent with the observations of Judge James Crawford, writing extra-judicially, that "*the principle of self-determination normally takes the well-known form of the rule preventing intervention in the internal affairs*

---

[44] Rule 66, paragraph 24.

[45] Commonwealth of Australia, Department of Foreign Affairs and Trade, Australia's International Cyber and Critical Technology Engagement Strategy, 2021, Annex B.

[46] *Foreign Cyber Interference* at p.754.

of a State".[47] Respondent will argue that it did not *deprive* the Suthan people of their right to vote or to choose their political status.

6.3.6 A Note on Funding by the Ravarian Embassy and Art 41 VCDR

Applicant may also argue that the funding of SAD and SIP by the Ravarian Embassy violated Art 41 of the VCDR:

> *Without prejudice to their privileges and immunities, it is the duty of all persons enjoying such privileges and immunities to respect the laws and regulations of the receiving State. They also have a duty not to interfere in the internal affairs of that State.*

However, this is generally interpreted to address interference by diplomatic staff in the receiving State on their own initiative, not on the instructions of the sending State. As noted in *Diplomatic Law*:[48]

> *Where a diplomat on instructions made some statement or took some step which was regarded by the receiving State as interference in its internal affairs, the question was whether the sending State had locus standi in the matter—as it would if the treatment of its own nationals or relations between the two States were involved. The long-standing rule now reflected in Article 41.1, however, related to personal comments or activities by diplomats not made on instructions.*

Accordingly, Art 41 would not be implicated if the acts of the Ravarian Embassy and Ambassador Walters were on the direct instruction of the Ravarian government (¶37). Further, the funding of SAD and SIP were permitted under Antaran domestic law, as was confirmed by the Antaran criminal investigation (¶38).

6.3.7 Suggested Questions

Basic Questions	1. Has the ICJ or any other international tribunal ever applied the obligation of non-intervention in the context of cyberspace? 2. What is its value of the Tallinn Manual 2.0 as a source of law? 3. What are examples of matters which are within the exclusive domain of States? 4. What is the definition of "coercion"?
Advanced Questions	1. (For Respondent) Why, in principle, should this Court not accept that the obligation of non-intervention applies in cyberspace if it is of general application? 2. (For Applicant) Can this Court extend the obligation to the new field of cyberspace in the absence of widespread and uniform State practice and *opinio juris* sufficient to form a rule of CIL? 3. In considering whether there has been coercion, can the Court consider the cumulative effect of all of Respondent's steps, or must it assess each step individually? How does this compare to this Court's approach in the *Nicaragua* case?

[47] James Crawford, The Creation of States in International Law (2nd edn., OUP 2007), p.126
[48] *Diplomatic Law*, p.377.

	4. (For Respondent) What is the impact of the Treaty of Singapore on the presence or absence of "coercion" here?

7. QP3: SUSPENSION OF HUNLAND'S PANO ACCOUNT

7.1 Introduction

The primary issue in QP3 is whether Applicant's order to suspend Hunland's Pano account was in accordance with international human rights law, specifically freedom of speech under Article 19 of the ICCPR.

The Relevant Facts for QP3

- Hunland is a citizen of Respondent (¶13). However, he moved to Antara in the 1980s and is a permanent resident there. Hunland is a tenured professor in a Suthan university. He is a pro-independence advocate, is affiliated with and authored the manifesto for the SIP, and has the third largest following on Pano in the Peninsula (¶13).
- Leading up to the independence referendum, Hunland used his Pano account to make many pro-independence posts including some that could be considered 'fake news'. Pano's Civic Integrity and Election Team flagged 63% of his posts, which were then covered with a warning requiring users to click to see them (¶24). Some of his posts contained language calling on his followers to "fight". Others, including one stating that there were plans to turn the Kuvil Shrine into an amusement park, were later shown to be false (¶23).
- Indisputable evidence has shown that several of the posts were false.
- On 31 January 2021, Hunland staged an outdoor rally with 7,500 in attendance, in breach of Antaran COVID-19 related restrictions. Violence broke out and 225 people were injured while three died (¶25).
- In February 2021, Applicant's DPCA submitted a petition for a content takedown and user suspension order against Hunland's posts and account. Hunland prepared a written statement in response, which he posted on social media (¶26).
- On 15 February 2021, an Antaran judge, after taking into account Hunland's arguments, granted the takedown order for one year (¶27). The order was later extended for a further six months (*Clarifications*, ¶3). There is no dispute that the order was granted and extended in compliance with Applicant's domestic law.
- Pano complied with the order (¶27).
- Hunland tried to obtain an injunction against the order from Applicant's courts, but the application was denied for lack of standing (¶28). He filed suit in Zemin seeking to have the order set aside (as Pano is incorporated in Zemin), but the action was dismissed as under Zemin law, social media platforms are not liable for content moderation (¶28).

Relevant Sub-Issues for QP3

- Whether Respondent has standing to bring the claim on behalf of Hunland
- Whether Antara's restriction on Hunland's freedom of speech was justified under Art 19(3) ICCPR

7.2 Standing: Diplomatic Protection

Applicant teams may address the issue of whether or not Respondent has standing to assert claims on behalf of Prof. Hunland.

7.2.1 Applicant Arguments

Prima facie it would appear that the nationality requirement is satisfied as Hunland is a citizen of Respondent. However, Applicant may argue that this is precisely the sort of exceptional circumstance as in the *Nottebohm* case, insofar as there is no 'genuine link' between Hunland and the country of which he is only nominally a citizen.

In *Nottebohm*, the individual held Liechtenstein citizenship, but had only a tenuous link with the country to which he had made no more than a few brief visits. He had lived most of his life (34 years) in Guatemala. The ICJ held that he was not a national of Liechtenstein under international law because he lacked any "*genuine connection*" to that country.[49]

In this case, Applicant will rely on the following facts:

- Prof. Hunland is a permanent resident of Applicant;
- He has lived in Applicant since the 1980s (*i.e.*, about 41 years, more than the 34 years in *Nottebohm*);
- He has been involved in Applicant's affairs for his entire adult life (specifically, as an advocate for the independence of Sutha).

7.2.2 Respondent Arguments

Respondent will argue that, pursuant to Article 4 of the ILC's Draft Articles on Diplomatic Protection, the nationality requirement is satisfied as long as the individual lawfully possesses citizenship of the State attempting to exercise diplomatic protection, which is the case with respect to Hunland. Respondent may point specifically to paragraph 5 of the commentary to Article 4:

> *Draft article 4 does not require a State to prove an effective or genuine link between itself and its national, along the lines suggested in the Nottebohm case, as an additional factor for the exercise of diplomatic protection, even where the national possesses only one nationality. Despite divergent views as to the interpretation of the case, the Commission took the view that there were certain factors that served to limit Nottebohm to the facts of the case in question, particularly the fact that the ties between Mr. Nottebohm and Liechtenstein (the applicant State) were 'extremely tenuous' compared with the close ties between Mr. Nottebohm and Guatemala (the respondent State) for a period of over 34 years.*

This comment suggests that the ICJ did not intend to propose a rule of general applicability. Further, Respondent can point to the facts of the more recent *Diallo* judgement, where Mr. Diallo, a Guinean national

---

[49] *Nottebohm (Liechtenstein/Guatemala) (Preliminary Objection (Second phase), Judgment)* [1955] ICJ Rep 4.

who had lived in the DRC for 32 years, was nevertheless entitled to the diplomatic protection of Guinea, his country of citizenship.[50]

7.2.3 Suggested Questions

Basic Questions	1. What are the requirements for a State to exercise diplomatic protection over an individual? Where can these be found? 2. What is the status of the Draft Articles on Diplomatic Protection? 3. What is the test for "nationality" under international law?
Advanced Questions	1. (To Applicant) Has the ICJ or any international court or tribunal ever applied or approved of the reasoning in the *Nottebohm* case? 2. (To Respondent) How can the *Nottebohm* case be distinguished from the present facts?

7.3 Freedom of Speech: Art 19 of the ICCPR

This issue is centered on Art 19 ICCPR:

> *1. Everyone shall have the right to hold opinions without interference.*
>
> *2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*
>
> *3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary:*
>
> *(a) For respect of the rights or reputations of others;*
>
> *(b) For the protection of national security or of public order (ordre public), or of public health or morals.*

7.3.1 Applicant Arguments

Applicant will focus on Art 19(3) ICCPR, arguing that the restrictions are justified under this provision as they are "*provided by law and are necessary, (a) for respect of the rights or reputation of others; (b) for the protection of national security or of public order (order public), or of public health or morals*".

"Provided by Law"

The restriction must be "*provided by law*". To be characterised as a "*law*", the piece of legislation must be formulated with sufficient precision to enable an individual to regulate his or her conduct to comply with

[50] *Ahmadou Sadio Diallo (Republic of Guinea/Democratic Republic of the Congo)* [2010] ICJ Rep 639.

it.[51] Applicant may argue that the provisions under section 5(1)(b) PACA (Annex 1) are not formulated with such precision because of the broadly-worded definition of "election misinformation" as *"false or misleading allegations or statements of fact likely to alter or otherwise impact the outcome of an election, or to incite imminent lawless action in connection with such election."*

Here, the terms "*misleading allegations*" and "*likely to alter or otherwise impact*" are highly subjective, and do not provide sufficient guidance to someone potentially affected by them.

Legitimate Aim

A law may not confer unfettered discretion for the restriction of freedom of expression on those charged with its execution.[52] Separately, the aim to be pursued by the restriction must be legitimate. The Special Rapporteur concluded in her 13 April 2021 report that:[53]

> *Any limitation of disinformation must establish a close and concrete connection to the protection of one of the legitimate aims stated in article 19(3). The prohibition of false information is not in itself a legitimate aim under international human rights law.*

Here, Applicant will argue that the legitimate aim was for "public order". Hunland organised a rally on 31 January 2021 with over 7,500 attendees in violation of the Antaran COVID-19 restrictions (¶25). This rally turned violent and three people died, with several hundreds more sustaining injuries. Hunland repeatedly published falsehoods, stirring up religious sentiment including alleging that the Kuvil Shrine would be turned into an "amusement park" (¶23) and an inauthentic photograph of Antaran police beating a woman who was praying at the rally (¶25). Against the backdrop of the referendum, drawing such deep divisions along religious lines along with incitements to "fight" (¶23) (which arguably was "incitement to imminent lawless action"), there was a legitimate aim in restricting Hunland's account.

Any restrictions under Art 19(2) ICCPR are also not to be assessed by reference to a "margin of appreciation",[54] and when taken holistically may not "*put in jeopardy the right itself*". It is always the restrictions, and not the right, that must be justified.[55]

The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression concluded in her 13 April 2021 report that:[56]

> *[g]iven the fundamental importance of freedom of expression to democracy and the enjoyment of all other human rights and freedoms, international human rights law affords particularly strong protection to expressions on matters of public interest, including criticism of Governments and political leaders and speech by politicians and other public figures, and to media freedom. This does not mean that*

---

[51] See also No. 578/1994, de Groot v. The Netherlands, Views adopted on 14 July 1995.
[52] General Comment No 27; Special Rapporteur's 13 April 2021 Report at para 40.
[53] At para 40.
[54] General Comment No 34 at para 36; see also No. 511/1992, *Ilmari Länsman, et al. v. Finland*, Views adopted on 14 October 1993.
[55] General Comment No 34 at para 21.
[56] At para 42.

disinformation in the context of political speech can never be restricted, but that any such restriction requires a high threshold of legality, legitimacy, necessity and proportionality.

Accordingly, limitations on the freedom of speech will be less likely to be upheld if they restrict criticisms of political candidates and governments.

Necessity & Proportionality

Any restriction of freedom of speech must conform to strict tests of necessity and proportionality.[57] A restriction is not necessary if its goal could be achieved in other ways which do not restrict the freedom of expression.[58] A measure is proportionate if it is the least intrusive means of achieving the intended goal.[59] Proportionality must be present not only in the text itself but also in the manner by which administrative and judicial authorities apply the law.[60]

Applicant will likely argue that the order is justified for the following reasons.

First, it is **necessary** "*for respect of the rights or reputation of others*". Applicant may point to Article 20(2) ICCPR which provides that "*Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law*". Applicant will argue that Hunland's post, as found by the judge, persistently called for action and created a serious risk of violence. Applicant will likely rely on caselaw, including that of ICTR, discussing the threshold for "incitement to violence."

Second, it is **proportionate** because the period of takedown was only for one year at a time, which is reasonable in light of the two-year negotiation period after the referendum ends (¶9). The potential for violence would be very real while the results of the referendum are being given effect. Particularly, Applicant can point to the tensions that could arise surrounding sensitive issues such as access to the Kuvil Shrine by Velans in Antara.

Third, prior to issuing the content takedown and account suspension orders, Pano had tried other means of ensuring that Hunland's posts did not incite violence, *e.g.* by putting them behind a warning screen that required users to click through before proceeding (¶24). Despite this, the judge concluded that they posed a serious risk of incitement.

Fourth, Applicant may contend that the restrictions were **consistent with State practice**. For example, when Twitter removed former President Trump's posts and indefinitely suspended his account, the complaints by foreign leaders were not about the ban *per se* but about the fact that it was done unilaterally by the social media network with no scrutiny by a court. No State has argued that Twitter's decision violated former President Trump's internationally-protected human rights. The ban on his account is indefinite, while the order against Hunland had a duration of one year (although it was subsequently extended).

---

[57] General Comment No 34 at para 22; see also No. 1022/2001, Velichkin v. Belarus, Views adopted on 20 October 2005.

[58] General Comment No 34 at para 33; see also No. 359, 385/89, *Ballantyne, Davidson and McIntyre v. Canada.*

[59] General Comment No 34 at para 34; Special Rapporteur's 13 April 2021 Report at para 41.

[60] General Comment No 34 at para 34.

Furthermore, even in the Special Rapporteur's 13 April 2021 report in which certain States' social media regulation laws were flagged as potentially contrary to Art 19 ICCPR, this was on the basis that "*[u]nfettered discretion has been given to executive bodies without judicial oversight*"[61] (legislation in Malaysia and Singapore), that authorities were granted "*excessive discretionary powers to compel social media platforms to remove content that they deem illegal ... In effect [leading] to suppression of legitimate online expressions with limited or no due process or without prior court order*"[62] (Kenya, Pakistan and the Russian Federation), and that the laws "*force platforms to decide whether to remove content without judicial orders*"[63] (Latin America). But the Antaran law under which Hunland's Pano account was suspended did require a court order, which was in fact issued.

The parties may discuss the fact that the suspension order was addressed to Pano, and not to Hunland. Pano is a private company. Yet Hunland was permitted only a limited form of participation in the judicial challenge to the order. Arguably, this is inconsistent with Art 2 of the ICCPR, which requires States to insure that "any person whose rights or freedoms as herein recognized are violated shall have an effective remedy," with the right to be "determined by competent judicial, administrative or legislative authorities, or by any other competent authority provided for by the legal system of the State." Yet when Hunland sought to obtain an injunction against the order, his case was dismissed for lack of standing (¶28).

7.3.2 Respondent Arguments

On the merits, Respondent will rely specifically on Art 19(2) ICCPR, which provides for the:

> *freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice*

Respondent will likely argue that the right under Article 19(2) applies in the cyber context, because it refers to the freedom to "*impart information and ideas*" through "*any*" media of the individual's choice. This position does not appear to be controversial,[64] and the HRC has taken the position in its General Comment No 34 that the right applies to electronic and internet-based modes of expression.[65]

In the context of discourse pertaining to potential election interference, General Comment No 34 notes that the freedom of expression applies to political discourse[66] and discourse on public affairs,[67] even to expression that may be regarded as deeply offensive[68] (so long as it does not come under the exceptions in

---

61 At para 54.
62 At para 55.
63 At para 55.
64 See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc A/HRC/17/27 (2011) at [52]; Statement by Secretary Johnson on Cyber Attack on Sony Pictures Entertainment, (19 Dec 2014) ("It was also an attack on our freedom of expression and way of life")
65 At para 12.
66 See also No. 414/1990, *Mika Miha v. Equatorial Guinea*.
67 See also No. 1157/2003, *Coleman v. Australia*, Views adopted on 17 July 2006.
68 See also No. 736/97, *Ross v. Canada*, Views adopted on 18 October 2000.

Article 19(3)).[69] The freedom of the media to comment on public issues without censorship means that the public has a corresponding right to receive media output.[70]

The European Court of Human Rights, in interpreting the parallel provision in the European Convention on Human Rights, has stated that the freedom of expression, in essence, prohibits a government from restricting a person from receiving information that others may wish or may be willing to impart to him.[71] Recently, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, opined that: (i) the freedom of expression applies to online platforms;[72] and (ii) the freedom of expression applies to:[73]

> *all kinds of information and ideas, including those that may shock, offend or disturb, and irrespective of the truth or falsehood of the content. Under international human rights law, people have the right to express ill-founded opinions and statements or indulge in parody or satire if they so wish*

In this case, Respondent may argue that requiring Prof. Hunland to take down not only his posts but his entire account was *prima facie* a disproportionate restriction of his freedom to impart information. Ravaria may go further to contend that the order interfered with the public's corresponding right to receive that information, although those allegedly deprived of that material were principally Antaran nationals, whom Ravaria has no standing to represent.

7.3.3 Suggested Questions

Basic Questions	1. What is the status of a General Comment issued by the Humans Right Committee? 2. Is there evidence on the record to show that Prof. Hunland's posts incited violence? 3. (To Applicant) What are the requirements for the exceptions under Article 19(3) ICCPR?
Advanced Questions	1. (To Applicant) Does State practice support the forced suspension of social media accounts by governments and the takedown of social media posts on political topics? 2. (To Respondent) Can Prof. Hunland's posts be classified as political discourse and/or discourse on public affairs? 3. (To Respondent) What is the relevance, if any, of the suspension and takedown order having a limited duration? 4. (To Respondent) What is the relevance, if any, of the fact that most of the suspension period was subsequent to the Referendum? 5. (To Respondent) What is the relevance, if any, of the fact that Pano had attempted to 'screen' Prof. Hunland's posts before Applicant issued the suspension and takedown order? 6. (To Applicant) What is the relevance, if any, of the fact that the suspension order was addressed to Pano, a private corporation, and not Prof. Hunland? 7. (To Respondent) What does Respondent say are the other alternative measures to which Applicant should have resorted before issuing the suspension order?

[69] At para 11.
[70] At para 13.
[71] *Leander v Sweden*, App no 9248/81, 9 EHRR 433, at para 74, (26 March 1987).
[72] At para 37.
[73] At para 38.

	8. Was the reach of the suspension order – encompassing all of Prof. Hunland's posts rather than only those of an arguably political character – disproportionate to any legitimate aim of the State?

8. QP4: LEGALITY OF APPLICANT'S BOTNET TAKEDOWN ORDER

8.1 Introduction

The issue in QP4 is whether Applicant's order to take down the Lunar Botnet violated international law, and specifically, whether it was an impermissible exercise of extraterritorial enforcement jurisdiction, given that roughly 5,000 of the hacked devices were located in Respondent's territory. (It is undisputed that the order was obtained in compliance with Applicant's domestic law.)

The Relevant Facts for QP4

- A 'botnet' is a network of devices infiltrated by malware which allows the botnet 'master' to control them. In this case, the Lunar Botnet infected over 30,000 devices over three months leading up to the Referendum and used them to spread misinformation relation to the vote (¶31).
- One week before the Referendum, Applicant's DPCA obtained a court order for the takedown of the Lunar Botnet ("Operation Moonstroke"). The Botnet was disabled on 26 February 2021, by removing the malware script ("web shells") from the infected devices (¶32). At the time of the takedown, the locations of the devices containing the botnet were unknown (*Clarifications*, ¶5).
- After the takedown, it was established that about 5,000 of the 30,000 infected devices were located in Respondent's territory.
- Respondent maintains that Operation Moonstroke was an impermissible act of extraterritorial enforcement. Applicant alleges that it was lawful and indeed necessary and that in cyberspace, territory can become irrelevant (¶33-34)

Pursuant to the *Lotus* decision, Applicant will have to justify its exercise of extraterritorial enforcement jurisdiction "*by virtue of a permissive rule derived from international custom or from a convention*".[74]

Relevant Sub-Issues for QP4

- Whether Respondent's claim is barred by the doctrine of clean hands
- Whether Applicant breached the Budapest Convention
- Whether Applicant breached customary international law
- Whether Applicant can raise any circumstances precluding the wrongfulness of the takedown order under the law of State responsibility

[74] *The Case of the SS Lotus (France v Turkey) (Judgment)* (1927) PCIJ Rep Series A No 10.

8.2 Clean Hands Doctrine

8.2.1 Applicant Arguments

Applicant may rely on the doctrine of clean hands, which was described by the PCIJ in *River Meuse* as follows:[75]

> *It would seem to be an important principle of equity that where two parties have assumed an identical or a reciprocal obligation, one party which is engaged in continuing non-performance of that obligation should not be permitted to take advantage of a similar non-performance of that obligation by the other party. The principle finds expression in the so-called maxims of equity which exercised great influence in the creative period of the development of Anglo-American law …. '[A] court of equity refuses relief to a plaintiff whose conduct in regard to the subject-matter of the litigation has been improper'. A very similar principle was received into Roman Law …. The* exceptio non adimpleti contractus *required a claimant to prove that he had performed or offered to perform his obligation*

The doctrine was restated in the Dissenting Opinion of Judge Schwebel in *Nicaragua*:[76]

> *Nicaragua has not come to Court with clean hands. On the contrary, as the aggressor, indirectly responsible—but ultimately responsible—for large numbers of deaths and widespread destruction in El Salvador apparently much exceeding that which Nicaragua has sustained, Nicaragua's hands are odiously unclean. Nicaragua has compounded its sins by misrepresenting them to the Court. Thus both on the grounds of its unlawful armed intervention in El Salvador, and its deliberately seeking to mislead the Court about the facts of that intervention through the false testimony of its Ministers, Nicaragua's claims against the United States should fail*

In *Certain Iranian Assets*, the ICJ did not expressly take a position on the clean hands doctrine. However, it noted that even if Iran's conduct was "not beyond reproach, this would not be sufficient per se to uphold the objection to admissibility" raised by the United States.[77]

Here, Applicant's objection to Respondent's claim is on the basis that the botnet itself was a violation of international law (the subject of QP2), attributable to Ravaria. Assuming that Applicant is successful in this claim, the clean hands doctrine would preclude Respondent from alleging that the takedown was illegal.

8.2.2 Respondent Arguments

Respondent may argue that this doctrine has never been conclusively accepted and applied in any ICJ decision. To the contrary, "clean hands" has been rejected by some international tribunals. For example, in *Yukos Universal Limited (Isle of Man) v The Russian Federation*, UNCITRAL, PCA Case No AA 227, Final Award, 18 July 2014, the Tribunal noted that despite Judge Schwebel's Dissenting Opinion in

---

[75] *The Diversion of Water from the Meuse (Netherlands/Belgium) (Individual Opinion of Judge Hudson)* [1937] PCIJ Rep Series A/B No 70 at para 77.

[76] *Nicaragua (Dissenting Opinion of Judge Schwebel)*, paras 268-272.

[77] *Certain Iranian Assets (Iran/USA) (Judgment on Preliminary Objections)* [2019] ICJ Rep. 7 at para 122.

Nicaragua, there has been no case in which the doctrine has actually been applied to bar a claim. Accordingly, the Tribunal concluded that the doctrine "*does not exist as a general principle of international law*".[78]

8.3 Budapest Convention

The parties are likely to discuss the Budapest Convention. The inclusion of extensive excerpts from that document is for the convenience of judges. It is not intended to suggest that these arguments should be the subject of focus, and indeed it may be challenging for Applicant to make a persuasive argument on this basis, for reasons set out below.

The 2001 European Convention on Cybercrime (the "**Budapest Convention**") was enacted to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation".[79] As noted in the Explanatory Report:[80]

> *The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation*

As stated in the Cybercrime Convention Committee's Guidance Note on the relevant provisions of the Convention, the use of botnets can amount to a breach of municipal law as provided for in Arts 2 – 8.[81] However, these Articles require contracting states only to "*adopt such legislative and other measures as may be necessary to establish [such acts] as criminal offences under its domestic law*".

The Budapest Convention also lays out several procedural issues in Section 2 of Chapter II and provisions relating to international cooperation in Chapter III:

> *Article 19 – Search and seizure of stored computer data*
>
> 1. *Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:*
>
> *(a) a computer system or part of it and computer data stored therein; and*
> *(b) a computer-data storage medium in which computer data may be stored in its territory.*
>
> 2. *Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to*

[78] At paras 1361-1636.
[79] *Preamble*, Budapest Convention.
[80] Explanatory Report to the Convention on Cybercrime, p.4.
[81] Cybercrime Convention Committee (T-CY) Guidance Note 2 on provisions of the Budapest Convention covering botnets (4-5 June 2013).

paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Article 22 – Jurisdiction

1. *Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:*

   (a) in its territory; or
   (b) on board a ship flying the flag of that Party; or
   (c) on board an aircraft registered under the laws of that Party; or
   (d) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. *Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.*

3. *Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.*

4. *This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.*

5. *When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.*

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

(a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
(b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 39 – Effects of the Convention

3. *Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.*

Art 19(2) of the Budapest Convention applies only within a State's own territory, and does not provide for extraterritorial jurisdiction. This is clear from both its ordinary meaning and the Explanatory Report: [82]

> *192. The reference to "in its territory" is a reminder that this provision, as all the articles in this Section, concern only measures that are required to be taken at the national level.*
>
> *193. Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory'.*

While some contracting States to the Budapest Convention have implemented extraterritorial enforcement jurisdiction in domestic statutes (as Antara has), not all have done so. Accordingly, there is no general State practice that "*establishes the agreement of the parties regarding its interpretation*" as required by Art 31(3)(b) of the Vienna Convention on the Law of Treaties.

In any event, Art 19 of the Budapest Convention includes only an obligation to "adopt … legislative measures". This is in line with the purpose of the Budapest Convention – to harmonise domestic legislation on cyber-crime. Nor does Art 22 provide for extraterritorial jurisdiction: it too only requires contracting States to enact laws that establish jurisdiction over crimes committed on its territory or by its nationals.[83]

Art 32 outlines the only two instances where a contracting State may access devices outside of its territory: (1) where such data is publicly available or (2) where lawful consent is given. As noted in the Explanatory Report:[84]

> *There was detailed consideration of instances in which it may be acceptable for States to act unilaterally and those in which it may not. The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules. Ultimately, the drafters decided to only set forth in Article 32 of the Convention situations in which all agreed that unilateral action is permissible. They agreed not to regulate other situations until such time as further experience has been gathered and further discussions may be held in light thereof. In this regard, Article 39, paragraph 3 provides that other situations are neither authorised, nor precluded.*

Accordingly, the Budapest Convention does not permit contracting States to take extraterritorial enforcement action.

---

[82] Explanatory Report to the Convention on Cybercrime, paras 192-193.
[83] Explanatory Report to the Convention on Cybercrime, paras 232-236.
[84] Explanatory Report to the Convention on Cybercrime, para 293.

8.4 Customary International Law

8.4.1 Applicant Arguments

As noted in the Tallinn Manual, "no consensus could be achieved as to whether, and if so, when, a cyber operation that results in neither physical damage nor the loss of functionality amounts to a violation of sovereignty".[85] Applicant may argue that Operation Moonstroke falls below the "loss of functionality" threshold.

The experts who argue that there is no such threshold rely on two bases: that a State is entitled to full control and access to activities on its territory, and that a State may not usurp an inherently governmental function that another State enjoys the exclusive right to perform.[86] Applicant will argue that neither of these considerations is relevant, especially given that the botmaster was located within Antara. It would not have been possible for Ravaria to disable the devices only on its own territory. And deletion of the malware could *never* have been carried out by the Ravarian government without access to the botmaster. Perhaps Antara could have notified Ravaria in advance, however, the DPCA was not aware that there were any devices outside of its territory when the botnet takedown order was sought (or issued).

Applicant may also argue that its acts are consistent with specific State practice regarding botnets. The Netherlands, for example, took down the foreign *Bredolab* botnet despite having previously stated that such acts were a violation of sovereignty.[87] Yet in a study titled "*Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*" commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs published in March 2017,[88] after a comparative analysis of EU and non-EU States, it was concluded that on the issue of territoriality, "*only one Member State, the Netherlands, legally permits the hacking of devices if the location is unknown. If the device turns out to be in another jurisdiction, Dutch law enforcement must apply for Mutual Legal Assistance.*"[89]

Applicant may also cite other domestic legislation or State practice that support the emergence of a norm permitting extraterritorial enforcement in cyberspace.

In a similar vein, although not specific to hacking or botnet takedowns, various countries have legislation under which the State can request information stored in servers outside their jurisdiction, including the US Clarifying Lawful Overseas Use of Data (CLOUD) Act and the People's Republic of China's National Intelligence Law.

---

[85] *Tallinn Manual*, Rule 4, para 14.

[86] *Tallinn Manual*, Rule 4, para 14.

[87] See further State practice and examples in A. Lubin, ' The Prohibition on Extraterritorial Enforcement Jurisdiction in the Datasphere' (2022) Handbook on Extraterritoriality in International Law (Austen L. Parrish and Cedric Ryngaert eds., forthcoming, 2022).

[88] *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices* at p.29.

[89] This incident of hacking into a server with an unknown location took place in 2014, where the Dutch Prosecution, as part of a large-scale investigation into the Blackshades malware coordinated by Eurojust, entered the server of Blackshades without knowing the location of the server on the basis of Article 125(i) of the Dutch Code of Criminal Procedure. At p.11.

States have also in practice used cyber investigative techniques even where it would likely impact persons outside their jurisdictions. In 2015, for example, the US FBI received intelligence that a website hosted on the "Tor" hidden service (not on the 'open' Internet) was distributing child pornography. A judge granted a warrant authorising a network investigative technique (NIT) to hack over 1,000 computers that visited the site over a 13-day period. The NIT permitted by the warrant was not limited geographically and could have applied to any visitor to the website regardless of location. It was reported that the NIT affected persons in Denmark, Greece and Chile.[90] However, none of these States (and indeed, no State in the international community) took the position that this was internationally wrongful.

In 2016, Australian authorities also reportedly used phishing attacks to bypass "Tor" software as part of a child pornography investigation, and in so doing hacked a computer in Michigan. The information was provided to the FBI.[91] Neither the US nor any other State argued that this was illegal. Given these and other examples. Applicant may argue that State practice has emerged permitting the exercise of extraterritorial enforcement jurisdiction in this manner.

In addition to citing State practice, Applicant may argue that its Operation Moonstroke is consistent with its exercise of other bases of jurisdiction under international law.

Protective principle: Applicant may rely on the protective principle insofar as the botnet threatened the vital interests of the State, since it was programmed to influence the referendum. However, there has been limited to no support for invoking this basis of jurisdiction to support extraterritorial enforcement jurisdiction in respect of either cyber activities generally or botnet takedowns specifically.

Passive personality: Applicant may contend that the victims of the botnet were its own citizens (the misinformation was aimed at them), justifying the exercise of enforcement jurisdiction on the basis of the passive personality doctrine.

8.4.2 Respondent Arguments

First, Respondent will argue that there is no loss of functionality threshold, so that even if Operation Moonstroke did not affect the functioning of devices in Ravaria, that does not affect its essential illegality. As noted in the Tallinn Manual in relation to botnet takedowns:[92]

> *if one State conducts a law enforcement operation against a botnet in order to obtain evidence for criminal prosecution by taking over its command and control servers located in another State without that State's consent, the former has violated the latter's sovereignty because the operation usurps an inherently governmental function exclusively reserved to the territorial State under international law*

Here, Respondent will assert that carrying out Operation Moonstroke without the consent of Ravaria usurped an inherently governmental function in relation to devices within its territory.

---

[90] At p.29.
[91] At p.29.
[92] *Tallinn Manual*, Rule 4, para 18.

Second, Respondent may argue that Applicant violated the principle of sovereignty by exercising extraterritorial enforcement jurisdiction over devices located within its territory and that no customary international law rule permits such an exercise.

Respondent will argue that claims like this have not been adjudicated before any international Court. The fact that States have engaged in cooperative exercises to take down botnets suggests that they acknowledge that their jurisdiction is otherwise territorially limited. For example, Respondent may point to the takedown of the *Ramnit* botnet in 2015 which involved cooperation from authorities from Germany, Italy, the Netherlands and the United Kingdom,[93] or of the *Emotet* botnet in 2021 undertaken by the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine.[94]

Objective territoriality doctrine / 'effects' doctrine: Respondent may argue that applying these doctrines to cyberspace would result in a destabilisation of the international legal order, as multiple States could claim jurisdiction over any particular cyber act where its effects are likely to be felt in many different States. Such an extension, if permitted at all, should be confined to specific areas such as antitrust law (where the US and other countries have applied the effects doctrine).

8.4.3 Suggested Questions

Basic Questions	On the issue of extraterritorial jurisdiction 1. What are the bases on which a State may exercise its enforcement jurisdiction outside its own territory? 2. Whose burden is it to show that there exists either a prohibitory or permissive rule regarding Applicant's exercise of extraterritorial jurisdiction? 3. Has the principle of sovereignty been applied in the context of cyberspace by the ICJ or any international tribunal? On the doctrine of clean hands 4. What are the requirements for the doctrine of unclean hands to apply? 5. What would be the result of a finding that Respondent has come to the Court with unclean hands?
Advanced Questions	On the issue of extraterritorial jurisdiction (a) (For Respondent) Given that cyberspace does not have physical boundaries, how can the principle of sovereignty, which is based on territory, be applied? (b) Apart from dicta in the *Lotus* case, have there been any decided cases in which the ICJ has recognised or applied the 'effects' doctrine? On the doctrine of clean hands

[93] https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation.

[94] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

	(c) Has the ICJ or any international court or tribunal ever applied the doctrine of unclean hands? (d) From which source of law does the doctrine of clean hands derive?