CyCon 2024: Over the Horizon
16th International Conference on Cyber Conflict
C. Kwan, L. Lindström, D. Giovannelli, K. Podiņš, D. Štrucl (Eds.)
2024 © NATO CCDCOE Publications, Tallinn

Not All Those Who Wander (Over the Horizon) Are Lost: The Applicability of Existing Paradigms of International Law to Cyberspace and the Interpretation of Customary International Law

Kristy Chan
LLM Candidate
University of Cambridge
BA Jurisprudence (Oxon)
kristychanwork@gmail.com

Joseph Khaw
BCL Candidate
University of Oxford
BA Jurisprudence (Oxon)
josephwykhaw@gmail.com

Abstract: It may be considered banal at this point for a State to assert that 'international law applies to cyberspace'. However, this belies tricky methodological questions regarding how a 'new' rule of customary international law (CIL) emerges. Cyberspace poses unique difficulties for the identification of CIL because of a paucity of publicly known State practice, vague statements, and attribution difficulties. However, this does not render CIL irrelevant to cyberspace. We argue that as the pace of technological development increases, interpretation of general rules of CIL may be used to ascertain their content when applied in cyberspace.

First, the proposed interpretive method is discussed. Second, State practice on the application of sovereignty and jurisdiction in cyberspace are considered to demonstrate interpretation in practice, focusing on extraterritorial botnet takedowns. Third, objections to the interpretive method are considered but shown to be ultimately unsustainable.

Normatively, the interpretation of CIL is an important tool for regulating cyberspace. First, it explains States' constant assertions that CIL applies to cyberspace despite the difficulties in meeting the usual tests. Second, on this approach, custom does not play catch-up to States' activities but develops contemporaneously. This allows

international law to peer over the horizon and be better prepared to tackle future challenges.

Keywords: *cyberspace, custom, identification, international law, interpretation, methodology*

1. INTRODUCTION

> *In their use of [information and communication technologies or ICTs], States must comply with international law … Hence, in current discussions, the question is no longer whether, but how international law applies to the use of ICTs by States.*[1]

> *Existing international law applies to cyber operations … Accordingly, the task of the International Groups of Experts … was to determine how such law applies in the cyber context.*[2]

This paper concerns methodology in customary international law (CIL). Specifically, if States think that international law applies in cyberspace, what does that mean from a methodological standpoint? *How* does a court work out what those rules are when applied? In what way, if at all, does that process differ from identifying a rule of CIL, which is 'to be looked for primarily in the actual practice and *opinio juris* of States'?[3]

We argue that applying existing international law to cyberspace can and should differ from identifying a new rule of CIL. Namely, it can be achieved through interpretation. Interpretation can help us look 'over the horizon' and enable custom to better address rapidly developing challenges in cyberspace, instead of playing catch-up. Ultimately, this article seeks to answer the call for Project 2100 through the domain of CIL,[4] strengthening custom as a tool for regulating cyberspace.

This paper proceeds in four sections. Section 2 explains our understanding of interpretation, its role in CIL methodology, and why cyberspace is a particularly

1 Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States, UNODA, A/76/136, August 2021, 17 (Brazil).

2 Michael Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017) 3 (*Tallinn Manual*).

3 *Continental Shelf (Libyan Arab Jamahiriya v Malta)* [1985] ICJ Rep 3 [27]; *North Sea Continental Shelf (Germany v Netherlands; Germany v Denmark)* [1969] ICJ Rep 3 [73].

4 See Sir Daniel Bethlehem KC, 'Project 2100 – Is the International Legal Order Fit for Purpose?' (*EJIL: Talk!*, 29 November 2022) <https://www.ejiltalk.org/project-2100-is-the-international-legal-order-fit-for-purpose/> accessed 6 January 2024.

ripe domain for applying the interpretive method. Section 3 applies interpretation to the rules of sovereignty in cyberspace, where State practice and *opinio juris* are sufficiently mature to deduce sub-obligations regarding extraterritorial botnet takedowns. Section 4 considers, but ultimately rejects, theoretical objections to interpretation. Section 5 concludes.

While this paper applies interpretation to sovereignty, the success of its broader argument regarding the potential of interpretation of CIL does not depend on accepting this example. Interpretation may be applied to various other aspects of international law in cyberspace. Nonetheless, space precludes comprehensive discussion of other areas.

2. WHAT IS INTERPRETATION?

A. Clearing the Field

Interpretation, as understood here, is a form of normative deduction in which 'new rules are inferred by deductive reasoning from existing rules and principles of CIL'.[5] This notion of 'interpretation' lies in the *application* of already recognized CIL to different factual matrices. While this process is guided by State practice and *opinio juris*, it is not the same as interpreting such practice itself. Understood this way, interpretation is irrelevant without an existing customary norm to be applied.

This might be confused with identifying the content of the existing norm, which critics of interpretation claim results in a vanishing line between identification and interpretation. Accordingly, interpretation allows courts to avoid the difficult requirement of establishing widespread and general State practice and *opinio juris*. Further, critics claim that customary rules do not exist in the abstract,[6] but are always tied to a particular context, such that 'identifying the content of the norm' and 'applying it to new contexts' are equivalent.

However, the relationship between the two is more like a Venn diagram. Interpretation and identification may overlap, and indeed in practice fleshing out the content of a rule as it applies in a new context looks the same as interpreting it to apply in a new context.[7] But in nascent areas such as cyberspace – where State practice and *opinio juris* are insufficient for the orthodox inductive methodology to bear fruitful results – interpretation and identification can produce different results. With knowledge of the

5 Stefan Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion' [2015] 26 EJIL 417, 423.

6 Massimo Lando, 'Identification as the Process to Determine the Content of Customary International Law' (2022) 42 OJLS 1042, 1049, 1051.

7 Dapo Akande, Antonio Coco, and Talita de Souza Dias, 'Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies' (2022) 99 Intl L Stud 4, 18: 'In practice, there is little difference between [the] process of custom-identification and the interpretation and application of general customary rules to new phenomena.'

rationale behind the rules as well as some State practice and *opinio juris*, interpretation can be used in situations where one might describe existing practice as 'rather sparse, owing to the relative newness of the question', thus 'preclud[ing] the possibility of those conditions arising which are necessary for the *formation* of principles and rules of customary law'.[8] The proviso 'necessary' may suggest that we are off to a non-starter. However, its focus is on the *formation* of *new* customary rules, which do not concern us. Instead, we are concerned with interpreting *existing* customary rules when *applying* them to new circumstances.

For example, in Section 3, we acknowledge that one could argue that interpretation and identification both define the 'content' of the norm of sovereignty as it applies in cyberspace. However, interpretation allows a court to answer *how* the rule of sovereignty applies in cyberspace, whereas identification (in the absence of the requisite State practice and *opinio juris*) cannot. Critically, this can only be achieved by relying on an existing rule.[9] In this case, that is the rule prohibiting interference with another State's territorial sovereignty.[10]

B. Interpretation as Gap-Filler

In this approach, interpretation and identification play different roles and do not supplant each other. Talmon suggests that the court apply deductive – or at least non-inductive – methods of reasoning when faced with new contexts.[11] Cyberspace, we argue, is one such context. Indeed, while Akande, Coco, and Dias suggest that cyberspace is merely a bundle of information technologies and not a different 'domain' at all,[12] they underplay the difficulties that are unique to identifying CIL in cyberspace that make interpretation critical. First, there is currently insufficient State practice and *opinio juris*, and what does exist is too inconsistent. Second, even if more practice and *opinio juris* arise in the future, cyber-specific difficulties arise from (i) a paucity of publicly available State practice, given the secrecy surrounding national technology; (ii) vague statements making *opinio juris* unclear; and (iii) difficulties in attributing conduct.[13] On (ii), while *opinio juris* has always been elusive,[14] its elucidation in

8 *Delimitation of the Maritime Boundary in the Gulf of Maine Area* (Canada v US) (Merits) [1984] ICJ Rep 246 [81].

9 Talmon (n 5) 441: 'Deduction is the logically consistent extrapolation of the established body of CIL. It is, however, important that new rules of CIL are deduced only from existing legal rules or principles and not from postulated values.'

10 *Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v Nicaragua) and Construction of a Road in Costa Rica along the San Juan River (Nicaragua v Costa Rica)* [2015] ICJ Rep 665 [93].

11 Talmon (n 5) 421–422.

12 Akande, Coco & Dias (n 7) 20.

13 Michael Schmitt and Stephen Watts, 'Collective Cyber Countermeasures' (2021) 12 HNSJ 373, 201–2; on attribution, see William Banks, 'Cyber Attribution and State Responsibility' (2021) 97 Intl L Stud 1039, 1046: 'Knowing the machines or IP addresses responsible for the hack is often difficult, costly, and time-consuming, and knowing those things does not necessarily lead easily to the responsible State.'

14 Omri Sender and Michael Wood, 'A Mystery No Longer? Opinio Juris and Other Theoretical Controversies Associated with Customary International Law' (2017) 50 Israel Law Review 299.

cyber contexts is even more difficult because of a lack of technical expertise from the actors to whom we usually turn to find *opinio juris*, such as State departments.[15]

Past instances of deductive reasoning by the International Court of Justice (ICJ) exhibit similar characteristics, as Talmon demonstrates.[16] This was the case where practice 'f[ell] short of proving the existence of a rule prescribing the use of equidistance, or any method, as obligatory',[17] as one might describe France's practice concerning botnet takedowns.[18] Similarly, in cases of negative practice consisting of omissions,[19] it may be 'practically impossible for one government to produce conclusive evidence of the motives which have prompted the action and policy of other governments'.[20] These considerations are all relevant in cyberspace.

One might question why a court should not just wait for further State practice and *opinio juris* to arise. First, as above, cyberspace is inherently inconducive to generating sufficient State practice and *opinio juris*. Thus, when a problem does come before the ICJ, unless the proposed methodological change is adopted, it may face a *non liquet*, which is 'no part of the Court's jurisprudence'.[21] Second, a critic might argue that there will be no *non liquet* if the closing rule in *Lotus* is applied: whatever is not prohibited is permitted.[22] However, as Hertogen has convincingly argued that *Lotus* does not stand for that proposition, the closing rule is of no help here.[23]

C. Interpretation as a Method of Legal Reasoning

But how can a court use interpretation to apply existing rules to new contexts? We propose the following elements of interpretation:[24] moving between levels of abstraction, teleological reasoning, and applying the rule.

15 Cf 'AI Safety Summit 2023' (GOV.UK) <https://www.gov.uk/government/topical-events/ai-safety-summit-2023> accessed 14 Apr 2024: The UK AI Safety Summit was intended to 'bring together international governments, leading AI companies, civil society groups and experts in research'. We agree that such events are valuable methods of elucidating more *opinio juris*, but we do not believe that it is sufficient given the quick pace at which novel technology in these fields develops.

16 *Gulf of Maine* (n 8) [81]; *Reparation for Injuries Suffered in the Service of the United Nations* [1949] ICJ Rep 174, 182 in Talmon (n 5) 422.

17 *Continental Shelf (Libya/Malta)* (n 3) [44].

18 Jack Kenny, 'France, Cyber Operations and Sovereignty: The "Purist" Approach to Sovereignty and Contradictory State Practice' (*Lawfare*, 12 March 2021) <https://www.lawfaremedia.org/article/france-cyber-operations-and-sovereignty-purist-approach-sovereignty-and-contradictory-state-practice> accessed 4 January 2024.

19 Paul C Ney Jr, 'DOD General Counsel Remarks at US Cyber Command Legal Conference' (*U.S. Department of Defense*, 2 March 2020) <https://www.defense.gov/News/Speeches/speech/article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/> accessed 7 January 2024: 'There is not sufficiently widespread and consistent State practice resulting from a sense of legal obligation to conclude that customary international law generally prohibits … non-consensual cyber operations in another State's territory.'

20 *North Sea Continental Shelf* (n 3) 246 (Dissenting Opinion of Judge Sørensen).

21 *Legality of the Threat or Use of Nuclear Weapons* (Advisory Opinion) (Dissenting Opinion of Judge Higgins) ICJ Rep 226 [36]; Talmon (n 5) 23.

22 *The SS 'Lotus'* 1927 PCIJ Series A, No 10, 18.

23 An Hertogen, 'Letting *Lotus* Bloom' [2016] 26 EJIL 901, 903.

24 Andreas Kulick, 'Interpreting the Customary Rules on State Responsibility – Text, No Text, Hypertext' in P Merkouris, P Pazartzis and LA Sicilianos (eds), *The Rules of Interpretation of Customary International Law* (CUP 2025, forthcoming) 9.

Critics such as Lando suggest that interpretation is not a viable method of legal reasoning as a matter of practicality because there are too many potential rationales.[25] However, as Talmon points out, the inductive method is 'just as subjective, unpredictable, and prone to law creation by the Court as the deductive method'.[26] Indeed, Tassinis convincingly shows that the orthodox method involves 'interpretation at every step of custom's life'.[27] Our focus, 'interpretation in application', is only one such step. Even Lando concedes that where State practice and *opinio juris* are lacking and courts have greater discretion, 'the case for the interpretability of custom, framed as a means to limit the exercise of discretion in determining the content of customary rules, might be more compelling'.[28]

Messiness is not inherently objectionable in international law. Kulick has pointed to the 'Eton messiness' of CIL as a defining feature of it,[29] while the International Law Commission (ILC) has described treaty interpretation as 'a single combined operation', whereby different means of interpretation are 'thrown into the crucible'.[30] This is what it means for interpretation to be a true *method*, as 'methods do not necessarily predetermine answers; they help explain how they are reached'.[31]

3. INTERPRETING RULES ON SOVEREIGNTY AND JURISDICTION TO APPLY TO CYBERSPACE

Consider an example: how do the customary prohibitions against infringing a State's territorial sovereignty and extraterritorial enforcement apply in the context of an extraterritorial botnet takedown?

For example, in the Anonymous Sudan botnet attack in November 2023, in which a Russia-backed group targeted networks in the US and Europe, any cross-border enforcement by States against Anonymous Sudan might be considered a breach of the targeted State's sovereignty. Thus, an attempt to 'delete' the webshells of a botnet attack – as States did during the takedown of EMOTET, which involved inserting malware into unknowing users' computers and initiating delete sequences[32] – would be considered an internationally wrongful act entailing State responsibility.

25 Lando (n 6) 1056.
26 Talmon (n 5) 432.
27 Orfeas Chasapis Tassinis, 'Customary International Law: Interpretation from Beginning to End' [2020] 31 EJIL 235.
28 Lando (n 6) 1046.
29 Kulick (n 24) 16; Section 4.
30 ILC, *Report on the Work of the Sixty-Eighth Session*, Subsequent Agreements and Subsequent Practice in Relation to the Interpretation of Treaties, Draft Conclusion 3(5) (UN Doc. A/71/10 (2016) 120).
31 Christian Tams, 'Self-Defence against Non-State Actors: Making Sense of the "Armed Attack" requirement' in Anne Peters and Christian Marxsen (eds), *Max Planck Trialogues on the Law of Peace and War* (CUP 2019) 93.
32 Daniel Rosenberg, 'Seizing the Means of Disruption: International Jurisdiction and Human Rights in the Expanding Frontier of Cyberspace' (2022) 55 NYU J Intl L & Pol 125, 143.

This is, however, at odds with current practice, where States hack into computers even where their location is unknown,[33] resulting in a potential breach of the victim State's sovereignty. States appear to have taken this uncertainty as a 'grant of jurisdiction', resulting in a 'new paradigm of enforcement jurisdiction'.[34] Further, not only are these operations announced *ex post facto*, kept quiet, or intentionally obfuscated such that *opinio juris* is difficult to find,[35] but State practice is also conflicting and disparate.[36] Even though many operations have highlighted their collaborative nature,[37] because the endpoint of the hack is not known until after the operation is conducted, acting States cannot claim to have obtained the victim State's consent.[38] This is exacerbated by the use of masking tools such as the dark web, which may obfuscate the true host of any botnets and hence render the 'endpoint' of the law enforcement agency's action unknown before conducting the cross-border operation.

Finally, existing treaties, such as the Budapest Convention, are of no help regarding botnets.[39] The Second Additional Protocol to the Convention on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224) does provide for 'emergency mutual assistance',[40] but the existence of a treaty rule does not itself preclude a customary rule on the same matter, though the treaty may contribute to the backdrop against which a particular customary rule is interpreted.[41]

This is not merely of academic interest: botnets have caused billions of dollars in damage[42] and implicate other extraterritorial enforcement operations against, for example, child pornography rings. While these might, like botnet takedowns, be benign acts that international law can choose not to regulate,[43] the lack of an international legal

33 ibid 144–48.
34 ibid 132, 142.
35 ibid 144.
36 See Kenny (n 18).
37 Office of Public Affairs of the US Department of Justice, 'Qakbot Malware Disrupted in International Cyber Takedown' (*U.S. Department of Justice*, 29 August 2023) <https://www.justice.gov/opa/pr/qakbot-malware-disrupted-international-cyber-takedown> accessed 9 March 2024.
38 Rosenberg (n 32) 148.
39 ibid 132: The Budapest Convention does not satisfactorily address extraterritorial enforcement of cybercrime laws and was drafted before the cloud era, when data was stored primarily in States' servers and not overseas, which fails to recognize the 'sheer mass of data transmitted across borders'. See also the Council of Europe's Explanatory Report and Guidance Notes (2022) at 305 on art 32b, suggesting that certain situations of transborder access of data by law enforcement officials are 'neither authorized nor precluded'.
40 Council of Europe, 'Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence' (2022).
41 Katie Johnston, 'The Nature and Context of Rules and the Identification of Customary International Law' (2021) 32 EJIL 1167.
42 Rosenberg (n 32) 127.
43 *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo* (Advisory Opinion) [2010] ICJ Rep 403, 478 (Opinion of Judge Simma) [9]: international law might be 'deliberately neutral or silent' on a particular issue, so 'an act might be tolerated [but that] would not necessarily mean that it is legal, but rather that it is not illegal'.

framework may result in 'the cure be[ing] worse than the disease'.[44] For example, States may abuse this to pursue 'active cyber defence'.[45]

A. Changing Levels of Abstraction

As a form of deductive reasoning, interpretation requires moving from the general to the specific. However, Pomson argues that because the ICJ has refused to apply abstract precedents to more specific circumstances, interpretation is unworkable.[46] This is to be rejected. First, it is not true that the Court never deduces obligations by applying abstract precedents to specific situations.[47] For example, Talmon points out that in *Corfu Channel*, the UK argued for the existence of a peacetime obligation using State practice during wartime as precedent.[48] The ICJ generalized 'up' from the wartime precedent to the more abstract principles, and then 'down' to apply it to the minefield peacetime situation.[49]

Second, Pomson's examples are cases where States have chosen to plead based not on the 'applicability' of law but on the need for an exception to the existing rule. Thus, in *Jurisdictional Immunities*, the ICJ confined its analysis to 'acts committed on the territory of the forum state by the armed forces of a foreign state', rather than examining general precedents regarding torts committed on the forum State's territory.[50] However, the way Italy and Germany pleaded their case – as an exception rather than a limitation – meant that 'the Court was not free to adopt whatever analytical approach it saw fit, for example by framing the existence of the territorial tort exception as the interpretation of an existing customary standard'.[51]

The same argument applies to Pomson's example of *Arrest Warrant*. Indeed, he points out that because 'Belgium focused on whether an exception for war crimes and crimes against humanity existing regarding the immunity ratione personae … the Court … was essentially responding … on the very terms of that argument'.[52] In other words, there was no room for the Court to consider more abstract precedents or rules. In fact,

44 Rosenberg (n 32) 141.
45 Jack Goldsmith and Alex Loomis, *'Defend Forward' and Sovereignty*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2102 (29 April 2021) <https://www.lawfareblog.com/defend-forward-and-sovereignty>.
46 Ori Pomson, 'Methodology of Identifying Customary International Law Applicable to Cyber Activities' (2023) 36 Leiden Journal Int'l Law 1023, 1041.
47 Talmon (n 5) 424: '[In *Corfu Channel*] the ICJ employed a triangular method of legal reasoning familiar in common law systems … where a precedent is similar to the case at bar in some important respects, but dissimilar in others, the [ICJ] identifies the general principles or rationale underlying the precedent and then decides whether this principle or rationale furnishes a suitable ground for deciding the case.'
48 ibid.
49 *Corfu Channel (UK v Albania)* [1949] ICJ Rep 4 [22].
50 *Jurisdictional Immunities (Germany v Italy)* [2012] ICJ Rep 99 [59].
51 Lando (n 6) 1052–53.
52 Pomson (n 46) 1037.

when it comes to State immunity, States have consistently framed their arguments in the form of exceptions to established rules.[53]

But if the perspective of States is what matters,[54] then this argument does not hold in cyberspace. States *do* view the content of norms from the top down and seek to establish how it applies in cyberspace, rather than seeking to establish a separate and parallel rule or an exception to the existing rule. The door is open to interpretation.

B. Teleological Reasoning

The next step is to determine whether the rationale for the main rule applies to the new situation. While Lando has argued that teleological reasoning is circular because the content of the existing general rule is itself the rationale, this is not true. This is because sovereignty and jurisdiction are residual rules of international law.

Residual rules are to be contrasted with norms such as humanitarian intervention, which operates as an exception to an existing rule. Here, CIL is not a 'micro-manager' but 'fills lacunae' when 'the diverse rules adopted by States collide'.[55] Thus, sovereignty is 'a residual rule that applies when no clear rule either prohibits or permits an action'.[56] It is up to the ICJ to decide this residual rule by considering the practice and the ultimate rationale of that area in question. In *Lotus*, the Court did not find that there was a 'presumption of freedom': it merely rejected a 'presumption against freedom', indicating that there may be limits on the exercise of sovereignty even when there is no express prohibition.[57] According to Hertogen, the rationale for this residual rule was that in the context of jurisdiction, 'territorial sovereignty must be exercised to ensure coexistence between independent States'.[58] The rule produced from this was that enforcement jurisdiction was prohibited unless a permissive exception could be established, such as consent.

It follows that when considering the applicability of sovereignty to cyberspace, the ICJ must continue to evaluate what is required for States to 'peacefully coexist', and it is *legitimate* to do so. According to *Lotus*, rules on enforcement jurisdiction are strictly controlled because of the horizontality of international law and the equality of States, regardless of size or history. Thus, the ICJ may start from the position that *any* infringement of territorial sovereignty entails a violation of sovereignty – that

53 Eg *Alleged Violations of State Immunities (Islamic Republic of Iran v Canada)* [2023] (ICJ proceedings instituted by Iran against Canada (27 June 2023), in which Canada argues for a 'terrorism' exception to State immunity).

54 Johnston (n 41) 1172: 'When the identification of [CIL] occurs in the context of litigation, much will therefore depend on how the issue is argued by the parties and how the rules involved are ultimately characterized by the Court … There does not appear to be any case before the ICJ where a party has succeeded in an argument relying on a customary rule that has been characterized as an exception to an existing customary rule.'

55 Hertogen (n 23) 911.

56 ibid 911.

57 ibid 908.

58 ibid 910.

is, identifying the existing rule. A court might choose to apply this *mutatis mutandis*, accepting that any intrusion into a State's cyberspace would result in a violation of its sovereignty. This would itself involve taking a stance on the rationale of the rules on sovereignty and jurisdiction – as the Permanent Court of International Justice did in *Lotus*. Alternatively, the ICJ may consider that the meaning of this changes given the porous nature of cyberspace and the need to address cybercrime in an increasingly interconnected world. In this approach, not *every* infringement of territory by cyber means entails violating the victim State's sovereignty.

C. Applying the Rule

However, the ICJ must choose between competing rationales and concretize the rule in application. This is the most controversial part of interpretation, especially compared to the inductive method, which assumes that one only needs to 'add up' State practice and *opinio juris*.[59]

For example, the ICJ may choose to adopt a 'de minimis' approach, where there is no violation of sovereignty if the effects of the State's hackback are minimal and the means used are the least intrusive. This is based on the need to ensure peaceful coexistence between States (the rationales outlined above), which, in a cyber context, necessitates some degree of jurisdictional overlap. However, Rosenberg has persuasively argued that this is only a good way of regulating an operation that has already taken place, and further restrictions are necessary to constrain State activities here.[60] Alternatively, the ICJ may consider that the absolute territorial prohibition is mirrored here and that any such hackback amounts to a violation of the hacked State's sovereignty. This may be motivated by considerations of undermining sovereignty in non-cyber domains.[61]

The point is that all of these interpretations are open to the ICJ – but it must choose, as it did in *Lotus* and *Nuclear Weapons*. In the latter, it evaluated existing practice and found that the general practice was prohibitory. Thus, proof of an exception – a permissive rule – had to be established, like in *Jurisdictional Immunities*. In cyberspace, the doors are wide open: it is more like *Lotus*, where Turkey and France disagreed on whether the content of sovereignty was permissive or prohibitive. It is

59 Moises Montiel, 'Fantastical Opinio Juris and How to Find It' (*Opinio Juris*, 23 June 2021) <https://opiniojuris.org/2021/06/23/fantastical-opinio-juris-and-how-to-find-it/> accessed 6 January 2024. Montiel argues that the two-element approach, where State practice and *opinio juris* is what CIL 'is', says nothing about how we get there; indeed, 'an equivalent would be saying that a cake is butter, flour, sugar, eggs, and milk. [This] is not wrong; but it adds nothing to the conceptual framework and hinders any attempt at identifying how to bake the coveted delicacy.'

60 Rosenberg (n 32) 153.

61 Consider, for example, the African Union Peace and Security Council's most recent statement rejecting a *de minimis* approach to sovereignty in cyberspace: Russell Buchan and Nicholas Tsagourias, 'The African Union's Statement on the Application of International Law to Cyberspace: An Assessment of the Principles of Territorial Sovereignty, Non-Intervention, and Non-Use of Force' (*EJIL! Talk*, 20 February 2024) <https://www.ejiltalk.org/the-african-unions-statement-on-the-application-of-international-law-to-cyberspace-an-assessment-of-the-principles-of-territorial-sovereignty-non-intervention-and-non-use-of-force/ > accessed 9 March 2024. As a bloc of 55 States, this should be considered strong State practice pointing away from a de minimis approach.

up to the ICJ to decide what approach to take, albeit based on a canvassing of practice in the area.

It should be noted that these terms ('effects', 'means', 'substantive') are taken from State practice and *opinio juris*, which, as cyberspace is such a technical domain, are used to *guide* the Court's application of the existing rule to formulate the new one, rather than being used in the usual inductive sense. Thus, our method of interpretation is still guided by State practice and *opinio juris*.[62]

4. IS THIS STILL CUSTOM?

It is admitted that this method of approaching custom, while not entirely *lex ferenda*, cannot be said to be *lex lata*. However, there are still normative benefits to adopting this method that outweigh potential objections.

A. Objection from Principle

Most vocal among these objections is that custom produced by interpretation is simply not custom at all. If custom is a 'practice' that has 'general acceptance as law', how can it be up to judges to specify 'what' that practice is if there is simply *no practice*? For example, Pomson argues that 'the proposition that customary rules are interpretable suggests … that one need not "always" have reference to state practice and *opinio juris* to determine the content of a customary rule'.[63] The criticism, then, is that interpretation impermissibly adds something to the mix that renders it 'not' custom.

However, first, there is practice given that we are advocating for interpretation to be used when States say that a general norm applies – interpretation is a way for the Court to specify *how*. Second, it is open to the international community to adopt a more fluid understanding of custom, such as that espoused by Hakimi,[64] where even an argument about what custom 'is' at a given moment on a particular topic counts as doing 'custom'. Interpretation fits well into this canon, though space constraints preclude further in-depth discussion.

62 *Barcelona Traction, Light and Power Company, Limited (Belgium v Spain)* [1970] ICJ Rep 3 (Separate Opinion of Judge Jessup) [60]: 'No survey of state practice can, strictly speaking, be comprehensive and the practice of a single State may vary from time to time … However, I am not seeking to marshal all the evidence necessary to establish a rule of [CIL]. Having indicated the underlying principles and the bases of the international law … I need only cite some examples to show that these conclusions are not unsupported by state practice and doctrine.'

63 Pomson (n 46) 1031–32.

64 Monica Hakimi, 'Making Sense of Customary International Law' (2020) 118 Michigan Law Review 1487; Jutta Brunnée, 'Customary International Law Symposium: Making Sense of Law as Practice (*Opinio Juris*, 7 July 2020) <https://opiniojuris.org/2020/07/07/customary-international-law-symposium-making-sense-of-law-as-practice-or-why-custom-doesnt-crystallize/> accessed 6 January 2024.

A related criticism is that interpretation allows what the law *ought* to be to determine what the law is. However, the Court is no stranger to attempting to ensure that CIL keeps pace with modern realities. For example, when arguing in favour of recognizing a right to self-defence against non-State actors,[65] Judge Kooijmans emphasized the need to make rules on the use of force suitable for modern dispute resolution – notwithstanding that this required departing from the mainstream interpretation of the past 40 years. In this approach, interpretation fills the gap between customary rules and the real-life scenario before the Court and allows CIL to develop contemporaneously with States' activities.

B. Objection from Practicality

Does interpretation make custom too uncertain? Especially as we advocate for interpretation to be used in nascent, developing areas of law, we acknowledge this potential uncertainty. Emerging custom would thus appear to reflect the words of US Supreme Court Judge Cardozo that 'the law that governs between [S]tates has at times … a twilight existence during which it is hardly distinguishable from morality or justice, till at length the imprimatur of a court attests its jural quality'.[66] However, the point is that interpretation avails itself when all that exists is the existing customary rule that States have said applies to cyberspace, which is arguably even more uncertain.

C. Objection from a Lack of Consent

The final potential objection is that this fails to respect the need for the consent of States, especially non-Western States. This cherry-picking of State practice and *opinio juris* to 'guide' interpretation renders interpretation nothing more than judicial legislation in disguise.[67]

Consent may indeed be lacking because States may object to whatever rule is produced from the interpretive process. However, because we advocate for interpretation to be used as a last resort when there is insufficient State practice, consent is only *potentially* lacking. There is room for States to object to such interpretations or for the persistent objector doctrine to apply.[68] Further, Talmon has persuasively argued that the deductive method is compatible with consent, given that deduction relies on the application of *existing* legal rules.[69] Nevertheless, from the perspective of Third

65 *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda)* [2005] ICJ Rep 168 [10]–[15].

66 *New Jersey v Delaware*, 291 US 361 (1934), in Rudolf Geiger, 'Customary International Law in the Jurisprudence of the International Court of Justice: A Critical Appraisal' in Fastenrath, Geiger, Khan, Paulus, von Schorlemer & Vedder (eds) *From Bilateralism to Community Interest: Essays in Honour of Bruno Simma* (OUP 2011) 673, 683.

67 Georg Schwarzenberger, 'The Inductive Approach to International Law' (1965) 60 Harvard Law Review at 126–27.

68 For example, the UK has always held that sovereignty cannot be breached as a standalone independent primary rule of international law.

69 Talmon (n 5) 441.

World approaches to international law (TWAIL), it is conceded that our methodology prioritizes *opinio juris* of States that have expressed a view on how international law applies to cyberspace, which will often be States of the Global North. However, this is reason for us to encourage further expression by States to generate more material for interpretation to work with,[70] rather than rejecting interpretation *per se*.[71]

The final charge – that interpretation is nothing more than judicial legislation – must be firmly rejected. First, it has always been true that many actors contribute to the articulation of substantive standards of conduct.[72] Thus, the legally binding status of international law may be *justified* by the consent of States to be so bound, but their content is not merely an expression of that will. Second, today's international legal order has 'radically transformed' as formal processes of international law-making have slowed.[73] While Pauwelyn focuses on the contribution of transnational corporations and nonprofits,[74] we suggest that *courts* can also be part of this change. As technology develops, we 'require more flexible norms … continuously corrected to take account of new developments'.[75] One way of doing so is to permit a more flexible CIL methodology that equips courts to play a greater part in law development.

5. CONCLUSION

Our argument is ambitious but limited. It is ambitious in that we suggest interpretation can help custom become fit for purpose in the 21st century. It is limited in that we propose great limits on it: the *type* of norm in question must be amenable to interpretation, requiring a nuanced understanding of differences between areas of international law. Given the difficulties posed by cyberspace to the development of CIL – including a lack of publicly available State practice, vagueness in national statements, and the significant technical expertise required to understand rapid technological developments – we argue that interpretation is necessary to look over the horizon.

70 In Episode 8 of the online podcast *Jus Cogens*, Eric Jensen, one of the original drafters of the *Tallinn Manual*, emphasizes that the goal was to put forward what the drafters believed *was* the law (lex lata) that would be material for States to respond to. See Dan Efrony and Yuval Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice' (2018) 112 AM J INT'L L 583, 588: 'The combination of silence and ambiguity in state practice and their reluctance to articulate their official policy in cyberspace prevents or, at least, slows the development of global norms of conduct.'

71 Jeffrey Kovar, 'The US' Practical Approach to Identifying Customary Law of Armed Conflict' (*EJIL: Talk!*, 21 August 2023) <https://www.ejiltalk.org/the-united-states-practical-approach-to-identifying-customary-law-of-armed-conflict/> accessed 6 January 2024.

72 ILC Draft Conclusions on the Identification of CIL (2018), Conclusion 4(3): '[The] conduct of other actors is not practice that contributes to the formation, or expression, of rules of customary international law, but may be relevant when assessing opinio juris.'

73 Joost Pauwelyn, Ramses Wessel and Jan Wouters, 'When Structures Become Shackles: Stagnation and Dynamics in International Lawmaking' (2014) 25 EJIL 733, 734.

74 ibid 741.

75 ibid 742–43.

Specifically, we argue that interpretation involves three stages: first, changing levels of abstraction; second, teleological reasoning; and third, applying the rule. Custom is not inherently opposed to any of these three stages. It is open for international law to choose interpretation as a methodology of CIL. However, on this approach, CIL does appear to be more interdisciplinary, less State-centric, and more contemporaneous. This is not to be rejected for fear of change. Indeed, 'the conceptual boundaries of how international law may look in the future are wide open'.[76] That surely includes methodological change.

76 ibid 734.