


ORIGINAL ARTICLE

INTERNATIONAL LAW AND PRACTICE

Election hacking, the rule of sovereignty, and deductive reasoning in customary international law

Steven Wheatley* 

Lancaster University Law School, Lancaster University, Lancaster, United Kingdom
Email: s.wheatley@lancaster.ac.uk

Abstract

This article considers the international laws applicable to irresponsible state behaviour in cyberspace through the lens of the problem of election hacking. The rule of sovereignty has taken centre stage in these discussions and is said to be preferred to the non-intervention rule because it evades the problem of coercion. Proponents of the cyber rule of sovereignty contend that there is such a rule; opponents reject the existence of the rule as a matter of existing law. The objective here is to explore the methodologies involved in the identification of the cyber rule of sovereignty under customary international law. The work first frames the debate in the language of regulative and constitutive rules, allowing us to show that a regulative rule of sovereignty can, logically, and necessarily, be deduced from the constitutive rule of sovereignty. The content of the regulative rule can also be deduced from the constitutive rule of sovereignty, but it has a more limited scope than claimed by the proponents of the rule, notably the Tallinn Manual 2.0. The rule of sovereignty prohibits state cyber operations carried out on the territory of the target state and remote cyber operations which involve the exercise of sovereign authority on that territory, e.g., police evidence-gathering operations. The rule of sovereignty does not, however, prohibit other remote, *ex situ* state cyber operations, even those targeting ICTs used for governmental functions, including the conduct of elections. The rule of sovereignty is not, then, the solution to the problem of election hacking.

Keywords: custom; cyber; deduction; election; sovereignty

1. Introduction

The political scientist, Joseph Nye makes the point that, just as sea power and air power opened up novel ways for states to achieve their foreign policy goals, the Internet and related information and communications technologies (ICTs) have created new opportunities for states to realize their foreign policy ambitions through the deployment of cyber power.¹ The open nature of democratic societies is said to place them at particular risk from malicious state cyber operations,² with much of the focus so far on the threats posed by information operations, where the objective is to change or reinforce the attitudes of citizens.³ This article, by way of contrast, focuses on the problem of

*Many thanks to the journal reviewers for their helpful and insightful comments.

¹J. S. Nye Jr., *Cyber Power* (2010), at 4.

²See, for example, Outcomes of the 'G7' meeting in Charlevoix, Canada, *Defending Democracy: Addressing Foreign Threats* (2018), available at www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-04-22-defending_democracydefendre_democratie.aspx?lang=eng.

³See, for example, T. van Benthem, D. B. Hollis, and T. Dias, 'Information Operations under International Law', (2022) 55 *Vanderbilt Journal of Transnational Law* 1217.

election hacking, defined as cyber operations that look to influence the outcome of a vote by targeting the ICTs used in the election. Real-world examples include distributed denial of service (DDoS) attacks on government websites,⁴ and the websites of political parties,⁵ to prevent them communicating with the public; removing people who have traditionally supported one party from the electoral roll;⁶ obtaining voter information and sending threatening messages concerning voting intentions;⁷ and even changing the outcome of the election by hacking the vote tabulation software.⁸

Whilst the dangers of election hacking are widely recognized, there is no consensus on the applicable international law rules. The standard way that international lawyers frame foreign state intermeddling in domestic politics is in terms of the non-intervention rule, which prohibits state cyber operations that use methods of coercion.⁹ The element of coercion is thought by some to create problems for the application of the non-intervention rule because coercion is often thought of in terms of a conscious unwilling act on the part of the victim.¹⁰ But this understanding does not translate easily to the cyber domain, where the target state is often unaware of the clandestine hacking of its ICTs. Whilst there are ways of understanding ‘coercion’ that do capture clandestine hacking operations,¹¹ the lack of agreement on the content of the cyber non-intervention rule has led scholars and policy makers to look elsewhere for limiting rules, including the individual right to political participation,¹² the collective right to (democratic) self-determination,¹³ and the cyber rule of sovereignty,¹⁴ found in Rule 4 of the Tallinn Manual 2.0., which would effectively prohibit all forms of election hacking (see below): ‘A State must not conduct cyber operations that violate the sovereignty of another State.’¹⁵

According to the Tallinn Manual, Rule 4 represents an objective statement of the current international law applicable to state cyber operations (the *lex lata*).¹⁶ This claim has resulted

⁴Huge Hack Attack on Bulgaria Election Authorities “Not to Affect Vote Count”, *Novinite.com*, 27 October 2015.

⁵D. A. Garcia and N. Torres, ‘Russia Meddling in Mexican Election: White House Aide McMaster’, *Reuters*, 7 January 2018.

⁶M. Calabresi, ‘Election Hackers Altered Voter Rolls, Stole Private Data, Officials Say’, *Time*, 22 June 2017.

⁷K. Collier, ‘Iran and Russia Deny FBI Accusation They Are Behind Threatening Emails Sent to Florida Democrats’, *NBC News*, 22 October 2020.

⁸N. Cheeseman and B. P. Klaas, *How to Rig an Election* (2018), at 104.

⁹*Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Merits, Judgment of 27 June 1986, [1986] ICJ Rep. 14, at 107–8, para. 205.

¹⁰K. Ziolkowski, ‘Peacetime Cyber Espionage: New Tendencies in Public International Law’, in K. Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy* (2013), 425, at 433 (‘Scholars assert that illegal coercion implies massive influence, inducing the affected State to adopt a decision with regard to its policy or practice which it would not entertain as a free and sovereign State.’).

¹¹S. Wheatley, ‘Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about “Coercion”’, (2020) 31 *Duke Journal of Comparative & International Law* 161.

¹²See, for example, B. Sander, ‘Democracy Under the Influence: Paradigms of State Responsibility for Cyber Influence Operations on Elections’, (2019) 18 *Chinese Journal of International Law* 1, para. 66 ff.

¹³See, for example, J. D. Ohlin, *Election Interference: International Law and the Future of Democracy* (2020), at 90; N. Tsagourias, ‘Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace’, in D. Broeders and B. van den Berg (eds.), *Governing Cyberspace: Behavior, Power, and Diplomacy* (2020), 45.

¹⁴See, for example, M. N. Schmitt, ‘Foreign Cyber Interference in Elections’, (2021) 97 *International Law Studies* 739, at 750 ff; also, P. C. R. Terry, ‘Voting by Proxy: Meddling in Foreign Elections and Public International Law’, (2022) 29(2) *Indiana Journal of Global Legal Studies* 67, at 106–7 (‘Some of the activities associated with election meddling are not only prohibited interventions in the internal affairs of another state but also violations of the target state’s sovereignty.’). Cf., however, J. D. Ohlin, *Election Interference: International Law and the Future of Democracy* (2020), at 75 (‘[I]nternational lawyers understand sovereignty in very particular ways, related to the prohibition on non-intervention, and its doctrinal requirements are a poor fit for evaluating election interference.’).

¹⁵M. Schmitt (ed.), NATO Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2017) (Tallinn Manual).

¹⁶‘Introduction’, in Tallinn Manual, *ibid.*, at 1, 3. See, generally, L. J. M. Boer, ‘Lex Lata Comes with a Date; Or, What Follows from Referring to the Tallinn Rules’, (2019) 113 *AJIL Unbound* 76, at 77.

in significant disagreement:¹⁷ supporters of the Tallinn Manual maintain that there is a rule of sovereignty, which applies equally in the cyber domain; opponents deny the existence of the cyber rule of sovereignty as a matter of existing law.

The question of responsible state behaviour in cyberspace has become the subject of ongoing discussions at the United Nations. There is general agreement that the rules of international law apply to the use of ICTs by states,¹⁸ but no consensus as to which rules apply, or how they apply. The final report of a UN Group of Governmental Experts (UNGGE) concluded that the non-intervention rule and human rights apply to state behaviour in cyberspace,¹⁹ but failed to affirm the existence of the cyber rule of sovereignty.²⁰ The search for agreement on the legal and normative framework for responsible state behaviour in cyberspace has now been remitted to an Open-ended Working Group on the use of ICTs,²¹ where the rule of sovereignty has again assumed a central place in discussions, but with no consensus emerging.²²

The objective of this article is to bring some clarity to these discussions by focusing on the methodologies involved in the identification of the existence and content of rules of customary international law. Section 2 outlines the debate on the status of the cyber rule of sovereignty. Section 3 considers the standard, inductive methodology involved in the identification of customary rules, explaining that a regulative rule of sovereignty cannot be inferred from the practices or policy positions of States. Section 4 shows that international lawyers also rely on deductive methodologies to determine the existence of custom – in this case, deducing the regulative rule of sovereignty from the constitutive rule of sovereignty. Section 5 considers the content of the rule of sovereignty, again by reference to a deductive methodology, showing that the cyber rule of sovereignty prohibits *in situ* state cyber operations and remote operations that usurp inherently governmental functions, but that the rule does not prohibit other remote state cyber operations targeting ICTs, including those that merely interfere with the exercise of inherently governmental functions.²³ The conclusion briefly summarizes the arguments, explaining why the rule of sovereignty is not the solution to the problem of election hacking.

2. Debating the rule of sovereignty

There are two kinds of international law rules: regulative rules and constitutive rules.²⁴ Regulative rules regulate the behaviours of states. They typically take the form of an imperative, ‘Do X’, or ‘Do not do X’.²⁵ Non-compliance with a regulative rule ‘breaks’ international law, entailing international responsibility. Constitutive rules, by way of contrast, allow for the creation of new institutional facts

¹⁷A. Assaf and D. Moshnikov, ‘Contesting Sovereignty in Cyberspace’, (2020) 1 *International Cybersecurity Law Review* 115, at 116 (‘The issue of sovereignty in cyberspace split the states and academia into two opposite camps.’).

¹⁸D. Akande, A. Coco and T. de Souza Dias, ‘Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies’, (2022) 99 *International Law Studies* 4, at 5 (‘In the past few years, the applicability of existing international law to cyberspace has received widespread and growing support among States.’).

¹⁹Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135 (2021), para. 70.

²⁰*Ibid.*, para. 71(b). The report does affirm that ‘international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities’: *Ibid.*

²¹The OEWG’s website is available at meetings.unoda.org/meeting/oewg-ict-2021/.

²²See member state views and inputs, available at meetings.unoda.org/meeting/57871/documents.

²³The focus of this article is state cyber operations, i.e., cyber operations attributable to the state. On the problems created by the architecture of the Internet for the attribution of state responsibility see N. Tsagourias, ‘Cyber Attacks, Self-Defence and the Problem of Attribution’, (2012) 17 *Journal of Conflict & Security Law* 229; L. Chircop, ‘A Due Diligence Standard of Attribution in Cyberspace’, (2018) 67 *International and Comparative Law Quarterly* 643.

²⁴On regulative and constitutive rules in law systems, generally, see A. Peczenik, *On Law and Reason* (1989), at 281.

²⁵J. R. Searle, ‘Constitutive Rules’, (2018) 4(1) *Argumenta* 51, at 51.

(i.e., facts of the international law system).²⁶ These include, for example, the institutional facts of ‘treaties’, the ‘High Seas’, and the ‘sovereign State’. Constitutive rules are typically expressed in terms that ‘X counts as Y (in context C)’.²⁷ Thus, an agreement concluded between states in written form and governed by international law counts as a treaty;²⁸ all parts of the sea not included in the territorial sea or exclusive economic zone count as the High Seas;²⁹ and some political communities count as sovereign states.³⁰ Failure to comply with the requirements of a constitutive rule does not ‘break’ the rule; it simply fails to create the new institutional fact.³¹ Thus, a political community that fails to meet the criteria of statehood does not ‘break’ international law by declaring its independence;³² it simply does not count as a sovereign state – for the purposes of international law.

The Tallinn Manual’s cyber rule of sovereignty is a claimed regulative rule of customary international law, in the form, ‘Do not conduct cyber operations that violate the sovereignty of another State.’³³ But the rule can also be expressed in a way that combines the regulative and constitutive rules of sovereignty: ‘A sovereign State must not conduct cyber operations that violate the sovereignty of another sovereign State.’³⁴

In other words, political communities which count as states (the constitutive rule of sovereignty) must not violate the sovereignty of other states (the regulative rule of sovereignty).

The notion of a regulative rule of sovereignty was initially met with scepticism, with opponents arguing that ‘sovereignty is a principle . . . rather than a hard and fast rule’.³⁵ The significance of the ‘sovereignty as rule’ *versus* ‘sovereignty as principle’ debate is not always clear,³⁶ although the principle of sovereignty appears to work as a placeholder for the moral or political standing of the state,³⁷ which in turn generates certain regulative rules (although the process of rule-generation is not explained), including the non-intervention rule.³⁸ The key dividing line in the literature is

²⁶C. Cherry, ‘Regulative Rules and Constitutive Rules’, (1973) 23 *Philosophical Quarterly* 301, at 303.

²⁷See Searle, *supra* note 25, at 52. Whilst the terminology of regulative and constitutive rules is widely used, scholars often employ the terms in different ways, with diverse views as to whether there is a category difference between regulative and constitutive rules, i.e., whether regulative rules can also constitute (see A. Giddens, *The Constitution of Society* (1984), at 19–20); whether constitutive rules can also regulate (J. Ransdell, ‘Constitutive Rules and Speech-Act Analysis’, (1971) 68 *Journal of Philosophy* 385, at 390); and whether a single rule can be both regulative and constitutive (J. Raz, *Practical Reason and Norms* (1975), at 109). In this article regulative and constitutive rules are narrowly and specifically defined, allowing for clear analytical insights, based on these understandings.

²⁸1969 Vienna Convention on the Law of Treaties, 1155 UNTS 331 (1969), Art. 2(1)(a). See, further, on this point, D. W. P. Ruiters, ‘Structuring Legal Institutions’, (1998) 17(3) *Law and Philosophy* 215, at 221 ff.

²⁹1982 United Nations Convention on the Law of the Sea, 1833 UNTS 3 (1982), Art. 86.

³⁰Once statehood is established, as James Crawford notes, the new state *is* sovereign, and whilst we use the term ‘sovereign state’, we might as well say ‘sovereign sovereign’: J. Crawford, ‘Sovereignty as a Legal Value’, in J. Crawford and M. Koskeniemi (eds.), *The Cambridge Companion to International Law* (2012), 117, at 117.

³¹See, generally, on this point, A. Dickey, ‘The Concept of Rules and the Concept of Law’, (1980) 25 *American Journal of Jurisprudence* 89, at 95.

³²See, on this point, *Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo*, Advisory Opinion of 22 July 2010, [2010] ICJ Rep. 403, at 438, para. 84 (‘[I]nternational law contains no applicable prohibition of declarations of independence.’).

³³See Tallinn Manual, *supra* note 15, Rule 4.

³⁴On the regulative and constitutive dimensions of sovereignty see, for example, D. Philpott, ‘Sovereignty: An Introduction and Brief History’, (1995) 48 *Journal of International Affairs* 353, at 358 (‘Rules of sovereignty are both “constitutive,” in defining the basic actors in the international community, and “regulative,” in specifying the rules which those actors must follow.’).

³⁵G. P. Corn and R. Taylor, ‘Sovereignty in the Age of Cyber’, (2017) 111 *AJIL Unbound* 207, at 210.

³⁶On the jurisprudential distinction between legal ‘principles’ and legal ‘rules’ see, classically, R. Dworkin, *Taking Rights Seriously* (1977).

³⁷N. Tsagourias, ‘The Legal Status of Cyberspace: Sovereignty Redux?’, in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (2021), 9, at 19.

³⁸N. Tsagourias, ‘Electoral Cyber Interference, Self-determination and the Principle of Non-intervention in Cyberspace’, in Broeders and van den Berg, *supra* note 13, at 47 (‘The importance of the principle of non-intervention derives from the fact that it emanates from and protects essential aspects of the principle of state sovereignty.’).

clear though: Some international law scholars, especially those specializing in the international law on cyber,³⁹ see sovereignty as a regulative rule, entailing international responsibility when the rule is broken.⁴⁰ Other international lawyers deny the existence of a regulative rule of sovereignty in the cyber domain as a matter of existing law.⁴¹

Proponents and opponents of the cyber rule of sovereignty disagree on the existence of the rule, on the relevance of the available state practice, and on the proper methodology for the identification of the customary rule of sovereignty.

On the existence of the cyber rule of sovereignty, proponents make the point that the International Court of Justice (ICJ) has, on several occasions, relied on a regulative rule of sovereignty to determine violations of international law.⁴² We see this, for example, in the *Corfu Channel* case, concerning the legality of a UK minesweeping operation, when the ICJ declared that the action of the British Navy ‘constituted a violation of Albanian sovereignty’.⁴³ Opponents respond by noting that the cases cited involved substantial military presence or de facto control of territory, and therefore ‘implicate higher thresholds than the [cyber] sovereignty-as-a-rule proponents assert’.⁴⁴

On the question of state practice, proponents highlight several instances which they claim support the existence of a regulative rule of sovereignty.⁴⁵ Notable cases include the 1960 ‘U2 incident’, when a US spy plane was shot down over Soviet airspace,⁴⁶ and, in the same year, Israel’s kidnapping of Adolf Eichmann in Buenos Aires.⁴⁷ Opponents are not convinced, with Gary Corn and Robert Taylor arguing that the proponents ‘look to sources dealing with very different domains and very different kinds of activities, and attempt to divine a rule where we see an absence of binding law’.⁴⁸

³⁹H. Lahmann, ‘On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace’, (2021) 32 *Duke Journal of Comparative and International Law* 61, at 66 (‘[M]ost international lawyers dealing with cyber issues . . . propose sovereignty as the obvious candidate.’).

⁴⁰See, for example, R. Buchan, *Cyber Espionage and International Law* (2018), at 49 (‘the rule of territorial sovereignty is firmly enshrined in customary international law’). See also W. H. von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’, (2013) 89 *International Law Studies* 123; B. Pirker, ‘Territorial Sovereignty and Integrity and the Challenges of Cyberspace’, in Ziolkowski, *supra* note 10, at 189; S. Watts and T. Richard, ‘Baseline Territorial Sovereignty and Cyberspace’, (2018) 22 *Lewis & Clark Law Review* 771; P. Roguski, ‘Violations of Territorial Sovereignty in Cyberspace: An Intrusion-based Approach’, in Broeders and van Den Berg, *supra* note 13, at 65; P. Pijpers and B. van den Bosch, ‘The “Virtual Eichmann”: On Sovereignty in Cyberspace’, (2020) Amsterdam Law School Research Paper No. 2020-65 (SSRN); K. J. Heller, ‘In Defense of Pure Sovereignty in Cyberspace’, (2021) 97 *International Law Studies* 1432; H. Lahmann, ‘Infecting the Mind: Establishing Responsibility for Transboundary Disinformation’, (2022) 33 *European Journal of International Law* 411. Also, D. Broeders et al., ‘Revisiting Past Cyber Operations in Light of New Cyber Norms and Interpretations of International Law: Inching towards Lines in the Sand?’, (2022) 1 *Journal of Cyber Policy* 97.

⁴¹See, for example, G. P. Corn, ‘Cyber National Security: Navigating Gray-Zone Challenges in and through Cyberspace’, in C. M. Ford and W. S. Williams, *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare* (2019), 345, at 417 (‘International law simply does not obligate other States to abstain from all nonconsensual activities within the territory of another State or that might otherwise infringe on or operate to the prejudice of that State’s internal sovereignty.’). Also, G. P. Corn and R. Taylor, ‘Concluding Observations on Sovereignty in Cyberspace’ (2017) *AJIL Unbound* 282, at 282; C. I. Keitner, ‘Foreign Election Interference and International Law’, in D. B. Hollis and J. D. Ohlin (eds.), *Defending Democracies* (2021), 179, at 191.

⁴²M. N. Schmitt and L. Vihul, ‘Sovereignty in Cyberspace’, (2017) 111 *AJIL Unbound* 213, at 215.

⁴³*Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania)*, Merits, Judgment of 9 April 1949, [1949] ICJ Rep. 4, at 35.

⁴⁴Corn and Taylor, *supra* note 35, at 207, 210.

⁴⁵M. N. Schmitt and L. Vihul, ‘Respect for Sovereignty in Cyberspace’, (2017) 95 *Texas Law Review* 1639, at 1656 (‘States have characterized a plethora of incidents as violations of their territorial sovereignty.’).

⁴⁶Q. Wright, ‘Legal Aspects of the U-2 Incident’, (1960) 54 *American Journal of International Law* 836, at 841.

⁴⁷The UN Security Council addressed the issue in terms of a ‘violation of sovereignty’, calling on Israel ‘to make appropriate reparation in accordance with . . . the rules of international law’: Security Council, Question relating to the case of Adolf Eichmann, Res. 138, S/4349 (1960). See L. C. Green, ‘The Eichmann Case’, (1960) 23 *Modern Law Review* 507, at 509 (‘An invasion by state agents . . . of the territory of another state constitutes a breach of the sovereignty of that state.’).

⁴⁸See Corn and Taylor, *supra* note 35, at 282.

On the question of methodology, proponents of the regulative rule do not look only to the available state practice and *opinio juris* to show the existence of a customary rule of sovereignty. The Tallinn Manual, for example, claims that a number of customary rules ‘derive from the general principle of sovereignty’,⁴⁹ including the rule that a state must not conduct cyber operations that violate the sovereignty of another state.⁵⁰ Opponents reject this deductive approach, with Jack Goldsmith and Alex Loomis contending that the Tallinn Manual adopts ‘an unorthodox method for identifying customary international law – so unorthodox . . . that it is entirely implausible that it reflects *lex lata*’.⁵¹

The objective here is to bring some clarity to these debates by focusing on the different methodologies involved in the identification of the existence and content of rules of customary international law. There are two ways this can be done (either alone or in combination): by way of induction, and by way of deduction.⁵² In the case of induction, we examine the available state practice and *opinio juris* to see if there is evidence of a general practice that is accepted as law; in the case of deduction, we deduce the existence of a customary rule from an existing rule, or from the constitutive rule of sovereignty. In all cases, we are looking for reasons to believe in the factual existence of a regulative rule – in this case the regulative rule of sovereignty (we are not talking about the creation of customary rules), with William Whewell explaining that ‘Induction moves upwards, and deduction downwards, [to meet] on the same stair.’⁵³ The two possibilities are considered in turn.

3. Identification of custom by way of induction

Article 38(1)(b) of the Statute of the International Court of Justice lists as one of the sources of international law, ‘international custom, as evidence of a general practice accepted as law’.⁵⁴ Whilst the provision is badly drafted, there is general recognition it outlines a two-element approach: to show the existence of custom, there must be (i) evidence of a general practice; and (ii) evidence of a belief the practice is required by international law (the *opinio juris* element).⁵⁵

Induction is central to the identification of custom,⁵⁶ because a customary rule, by definition, ‘is not written and has no “authoritative” text’.⁵⁷ In *Continental Shelf (Libya/Malta)*, the ICJ

⁴⁹See Tallinn Manual, *supra* note 15, Rule 1, Explanatory para. 3 (emphasis added).

⁵⁰*Ibid.*, Rule 4.

⁵¹J. Goldsmith and A. Loomis, ‘Defend Forward and Sovereignty’, (2021) A Hoover Institution Essay, Aegis Series Paper No. 2102, at 7.

⁵²See, on this point, Draft Conclusions on Identification of Customary International Law, with Commentaries, in Report of the International Law Commission, Seventieth session, UN Doc. A/73/10 (2018), Conclusion 2, Commentary, para. 5, at 126 (‘The two-element approach is often referred to as “inductive”, in contrast to possible “deductive” approaches by which rules might be ascertained other than by empirical evidence of a general practice and its acceptance as law (*opinio juris*). The two-element approach does not in fact preclude a measure of deduction as an aid, to be employed with caution, in the application of the two-element approach.’).

⁵³W. Whewell, *The Philosophy of the Inductive Sciences* (1947), vol. II, quoted C. Wilfred Jenks, *The Prospects of International Adjudication* (1964), at 658.

⁵⁴1945 Statute of the International Court of Justice, Art. 38(1)(b).

⁵⁵See, for example, *North Sea Continental Shelf (Federal Republic of Germany/Netherlands)*, Judgment of 20 February 1969, [1969] ICJ Rep. 3, at 44, para. 77 (‘Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of law requiring it.’).

⁵⁶The reliance on inductive methodology depends on deductive reasoning, a point the ICJ recognizes: See *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 9, at 88, para. 186 (‘In order to deduce the existence of customary rules, the Court deems it sufficient that the conduct of States should, in general, be consistent with such rules.’).

⁵⁷J. Kammerhofer, ‘Uncertainty in the Formal Sources of International Law: Customary International Law and Some of Its Problems’, (2004) 15 *European Journal of International Law* 523, at 524.

expressed the point this way: 'It is of course axiomatic that the material of customary international law is to be looked for primarily in the actual practice and *opinio juris* of States.'⁵⁸

In the same way that we infer the general physical law of gravity from empirical observations of apples always falling towards the ground, we infer the existence of 'contingent'⁵⁹ customary rules from the behaviours and utterances of states.⁶⁰

There are three steps in any inductive methodology: the collection of empirical, real-world data; an evaluation of that data, looking for patterns; and reaching a conclusion based on the evidence. Our conclusion will be compelling, or not, depending on the extent to which the data supports the conclusion. Arguments with significant confirmatory evidence are said to be strong; those without are said to be weak. The results of inductive reasoning cannot, then, be categorized as being 'true' or 'false' – only as being cogent or not cogent, depending on the extent to which the conclusion is supported by the data.⁶¹ The more empirical evidence in support of the conclusion, the more likely it is to be true – the so-called Bayesian hypothesis.⁶²

In relation to state practice, the inductive method directs us to the following: collect the available evidence of the practice of states;⁶³ evaluate that data, looking for patterns in those practices;⁶⁴ and reach a conclusion, based on the data, as to whether there appears to be a rule of appropriate conduct. Absolute conformity in the practice is not required, with the ICJ referring variously to the requirement for state practice to be 'virtually uniform',⁶⁵ or 'in general' consistent with the rule.⁶⁶

In relation to the claimed rule of sovereignty, there is limited state practice in the physical domain and no clear state practice in the cyber domain. Schmitt and Vihul have carried out the most detailed survey of state practice in the physical domain, but they find only five instances where the rule of sovereignty has been expressly invoked between states.⁶⁷ In relation to the cyber domain, the most detailed evaluation of state practice has been carried out by Dan Efrony and Yuval Shany, who detail several state cyber operations targeting ICTs in other states, including the Shamoon 1 cyber operation, blamed on Iran, which destroyed the hard drives of tens of thousands of computers in Saudi Arabia, and the WannaCry and NotPetya ransomware attacks,

⁵⁸*Continental Shelf (Libyan Arab Jarnahiriya/Malta)*, Judgment of 3 June 1985, [1985] ICJ Rep.13, at 29, para. 27.

⁵⁹Because we cannot predict the future actions and interactions of states, we cannot tell in advance what customary rules will emerge. Christian Tomuschat refers to this kind of customary international law as 'contingent custom'. See C. Tomuschat, 'Obligations Arising for States Without or Against their Will', (1993) 241 *Recueil des Cours* 195, at 307.

⁶⁰S. Talmon, 'Determining Customary International Law: The ICJ's Methodology between Induction, Deduction and Assertion', (2015) 26 *European Journal of International Law* 417, at 420 (the inductive method in customary international law 'may be defined as inference of a general rule from a pattern of empirically observable individual instances of State practice and *opinio juris*').

⁶¹R. D. Rosenkrantz, 'Does the Philosophy of Induction Rest on a Mistake?', (1982) 79(2) *Journal of Philosophy* 78, at 78.

⁶²See J. W. Moses and T. L. Knutsen, *Ways of Knowing: Competing Methodologies and Methods in Social and Political Research* (2007), at 260–1.

⁶³See International Law Commission, Draft Conclusion 6(2) on Identification of Customary International Law, annexed to General Assembly Res. A/73/203, 'Identification of Customary International Law', adopted 20 December 2018, without a vote ('Forms of State practice include, but are not limited to: diplomatic acts and correspondence; conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference; conduct in connection with treaties; executive conduct, including operational conduct "on the ground"; legislative and administrative acts; and decisions of national courts.').

⁶⁴See, generally, on the importance of patterns to international lawyers, P. Allott, 'Language, Method and the Nature of International Law', (1971) 45 *British Yearbook of International Law* 79, at 104.

⁶⁵See *North Sea Continental Shelf*, *supra* note 55, at 44, para. 74.

⁶⁶See *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 9, at 88, para. 186.

⁶⁷See Schmitt and Vihul, *supra* note 45, at 1656 ff. The instances of state practice where 'sovereignty' was expressly invoked between states were the 2001 EP-3 incident; US counterterrorist drone strikes in Pakistan; the 1960 Eichmann case; the Cosmos 954 satellite crash; and Russian military operations in Ukraine. See also, on the few instances of state practice, Heller, *supra* note 40, at 1439–40.

blamed respectively on North Korea and Russia, that infected computer systems all around the world. On the question as to whether there is evidence, in the practice of states, of a regulative rule of sovereignty, Efrony and Shany conclude that their case studies ‘do not fully clarify this point of contention’.⁶⁸ On the one hand, states do not claim a legal right to conduct malicious cyber operations and there have been some diplomatic complaints by victim states. On the other, the rule of sovereignty is not invoked by the target state in any of the cases they examined. Thus, for example, statements attributing responsibility to North Korea and Russia for the WannaCry and NotPetya operations ‘did not explicitly refer to infringements of sovereignty, or any specific rule derived thereof’.⁶⁹ Goldsmith and Loomis make the same point, concluding that in none of the state cyber operations they examined, ‘not a single one, have we found evidence that the victim state complained about a violation of a customary international-law rule of sovereignty’.⁷⁰

Along with evidence of state practice, the identification of custom requires evidence of a belief that the practice is accepted as law (*opinio juris*), allowing us to distinguish between customary international law rules and rules of appropriate behaviour complied with as a matter of political convenience.⁷¹ In simple terms, the patterns of states utterances must reflect the existence of a regulative rule expressed in terms of rights and duties.⁷² Again, the inductive method directs us to: collect the data on the verbal acts of states concerning the status of the rule, found, for example, in official publications;⁷³ evaluate the data, looking for a clear pattern in states utterances on the status of the rule; and reach a conclusion as to whether there is a regulative international law rule, whereby breaking the rule entails international responsibility.

The different positions on the status of the cyber rule of sovereignty can be categorized as follows: first, those states – notably the United Kingdom,⁷⁴ and United States of America⁷⁵ – who do not believe in the existence of a regulative rule of sovereignty; second, those states – like Peru,⁷⁶ and Russia⁷⁷ – who remain agnostic on the issue, i.e., have not taken a position when commenting on the rules applicable to cyber operations; third, those states who believe in the existence of the

⁶⁸D. Efrony and Y. Shany, ‘A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyber Operations and Subsequent State Practice’, (2018) 112 *American Journal of International Law* 583, at 640.

⁶⁹*Ibid.*, at 641.

⁷⁰See Goldsmith and Loomis, *supra* note 51, at 9.

⁷¹L. Oppenheim, *International Law: A Treatise* (1905), vol. I, at 23.

⁷²*Asylum (Colombia v. Peru)*, Judgment of 20 November 1950, [1950] ICJ Rep. 266, at 276.

⁷³See International Law Commission, *supra* note 52, Draft Conclusion 10(2) (‘Forms of evidence of acceptance as law (*opinio juris*) include, but are not limited to: public statements made on behalf of States; official publications; government legal opinions; diplomatic correspondence; decisions of national courts; treaty provisions; and conduct in connection with resolutions adopted by an international organization or at an intergovernmental conference.’).

⁷⁴S. Braverman, Attorney-General, ‘International law in Future Frontiers’, 19 May 2022, available at www.gov.uk/government/speeches/international-law-in-future-frontiers (‘The general concept of sovereignty, by itself, does not provide a sufficient or clear basis for extrapolating a specific rule of sovereignty or additional prohibition for cyber conduct, going beyond that of non-intervention.’). See also J. Wright, Attorney General, ‘Cyber and International Law in the 21st Century’, 23 May 2018, available at www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century (‘Sovereignty is of course fundamental to the international rules-based system. Although I am not persuaded that we can currently extrapolate from that general principle a specific rule.’).

⁷⁵P. C. Ney, Jr., ‘DOD General Counsel Remarks at U.S. Cyber Command Legal Conference’, 2 March 2020, available at www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference (‘[I]t does not appear that there exists a rule that all infringements on sovereignty in cyberspace necessarily involve violations of international law.’).

⁷⁶See D. B. Hollis, ‘International Law and State Cyber Operations: Improving Transparency’, CJI/doc. 603/20 rev.1 corr.1 (5 March 2020), para. 53 (Hollis Fourth Report).

⁷⁷Contribution of the Russian Federation on Rules, Norms and Principles of Responsible Behaviour of States in Information Space, para. 5, available at documents.unodc.org/wp-content/uploads/2022/03/Russian-contribution-on-rules-of-behaviour-Eng.pdf.

regulative rule of sovereignty – Austria,⁷⁸ Bolivia,⁷⁹ Canada,⁸⁰ Chile,⁸¹ Czech Republic,⁸² Estonia,⁸³ China,⁸⁴ Finland,⁸⁵ France,⁸⁶ Germany,⁸⁷ Guatemala,⁸⁸ Guyana,⁸⁹ Iran,⁹⁰ Italy,⁹¹ The Netherlands,⁹² New Zealand,⁹³ Sweden,⁹⁴ and Switzerland,⁹⁵ and, finally, the majority of states who have not expressed an opinion on the status of the cyber rule of sovereignty, notwithstanding the active discussions on the issue at the United Nations and elsewhere.

To show the factual existence of a rule of customary international law through inductive reasoning, we require sufficient evidence of state practice and *opinio juris* to conclude that the rule exists, limiting states behaviours. Reliance on an inductive methodology means that we cannot prove the existence of customary rules, only find good evidence for them. One consequence is that different international lawyers can come to different conclusions on the existence of a rule after considering the same evidence.⁹⁶ Proponents of the cyber rule of sovereignty have examined the available state practice and *opinio juris* and concluded that there is sufficient evidence to show a general practice that is accepted as law.⁹⁷ Opponents have looked at the same evidence and

⁷⁸Pre-Draft Report of the OEWG: ICT Comments by Austria, at 3, available at front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf.

⁷⁹See Hollis Fourth Report, *supra* note 76, para. 52.

⁸⁰Canada, 'International Law Applicable in Cyberspace', para. 15, available at www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_scurite/cyberspace_law-cyberspace_droit.aspx?lang=eng.

⁸¹See Hollis Fourth Report, *supra* note 76, para. 54.

⁸²Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace Director of Cybersecurity Department, at the 2nd Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security of the First Committee of the General Assembly of the United Nations, 11 February 2020, available at www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf.

⁸³Estonia, 'Estonian positions', available at documents.unoda.org/wp-content/uploads/2021/12/Estonian-positions-OEWG-2021-2025.pdf.

⁸⁴China's Views on the Application of the Principle of Sovereignty in Cyberspace', at 2, available at documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf.

⁸⁵'International Law and Cyberspace: Finland's National Positions', available at www.valtionuuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace.

⁸⁶France, 'International Law Applied to Operations in Cyberspace', at 2, available at documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

⁸⁷Germany, 'On the Application of International Law in Cyberspace', at 3, available at documents.unoda.org/wp-content/uploads/2021/12/Germany-Position-Paper-On-the-Application-of-International-Law-in-Cyberspace.pdf.

⁸⁸See Hollis Fourth Report, *supra* note 76, para. 52.

⁸⁹*Ibid.*

⁹⁰Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace', July 2020, Art. II(3), available at www.nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

⁹¹Italian position paper on "International law and cyberspace", at 4, available at documents.unoda.org/wp-content/uploads/2021/10/italian-position-paper-international-law-and-cyberspace.pdf.

⁹²The Netherlands, 'International Law in Cyberspace' (document sent by the Government of the Kingdom of the Netherlands to Parliament 5 July 2019, at 2, available at www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

⁹³New Zealand, 'The Application of International Law to State Activity in Cyberspace', para. 11, available at www.dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace.

⁹⁴Sweden, 'Position Paper on the Application of International Law in Cyberspace', at 2, available at documents.unoda.org/wp-content/uploads/2022/07/Position-Paper.pdf.

⁹⁵Switzerland, 'Position Paper on the Application of International Law in Cyberspace', Annex UN GGE 2019/2021, at 3, available to download at www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

⁹⁶P. H. Verdier and E. Voeten, 'Precedent, Compliance, and Change in Customary International Law: An Explanatory Theory', (2014) 108 *American Journal of International Law* 389, at 415 ('[D]ifferent states, international courts, and scholars often come to opposite conclusions after reviewing the very same practice.').

⁹⁷See Schmitt and Vihul, *supra* note 45, at 1650.

reached the opposite conclusion.⁹⁸ Neither determination can be categorized as true or false, only cogent or not cogent. However, the limited state practice in the physical domain and absence of clear state practice in the cyber domain, along with the divided positions of states, makes it difficult to accept the claim there is a general practice that is accepted as law. We cannot, then, based on an inductive methodology alone, show the factual existence of a rule of sovereignty.

4. Identification of custom by way of deduction

There are times when the ICJ looks to deductive reasoning in the identification of customary international law rules: customary rules are deduced from existing rules of customary international law, which themselves reflect a general practice that is accepted as law, and from the constitutive rule of sovereignty. The two possibilities are considered in turn,⁹⁹ after an explanation of the way that international lawyers use deductive reasoning.

4.1 Deductive reasoning by international lawyers

Deductive reasoning is the process of drawing a conclusion from what we already know and believe. There are typically two steps in the process: An evaluation of what we know and believe; and, drawing a novel conclusion, making explicit something implicit in what we already know and believe. The standard form of deduction is the *modus ponens*, a rule of logic in the form:

If P, then Q

P

Therefore Q.¹⁰⁰

A well-known example concerns the mortality of the Greek philosopher, Socrates: *If* Socrates is human, *then* Socrates is mortal; Socrates is human; Therefore, Socrates is mortal.

With deductive reasoning, we start with our knowledge and beliefs and produce a novel conclusion. The aim is to reach a valid conclusion which is true because our knowledge and beliefs are true. A conclusion is logically valid provided no mistakes have been made in the reasoning. But this does not guarantee the veracity of the conclusion. The veracity of the output conclusion (Q) depends on the veracity of the input premise (P) – *If* P, *then* Q. Valid deductive conclusions will be wrong if the input premise is wrong. Consider the following – logically valid – argument: *If* Socrates is human, *then* Socrates can fly; Socrates is human; Therefore, Socrates can fly. But Socrates cannot fly: This is a brute fact of the world. The fact I reason that Socrates can fly can be tested empirically and proved to be ‘false’.

International lawyers rely on deductive reasoning when they deduce new facts about the nature, scope or content of the international law system from their existing knowledge and beliefs (i.e., without gathering new empirical, real-world data – e.g., instances of state practice). But the facts of the international law system are different from the brute facts of the world (e.g., whether Socrates can fly, or not). Brute facts are true whatever we say or think about them; the facts of a social institution, like international law, by way of contrast, are only true because those who recognize

⁹⁸See Goldsmith and Loomis, *supra* note 51, at 13.

⁹⁹The ICJ has also recognized the possibility of deducing regulative rules from moral principles (see *Corfu Channel*, *supra* note 43, at 22) and from principles of equity (*Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain)*, Preliminary Objections, Judgment of 5 February 1970, [1970] ICJ Rep. 3, at 48, para. 94).

¹⁰⁰For an example of ‘If P, then Q’ reasoning applied to law see N. MacCormick, *Legal Reasoning and Legal Theory* (1978), at 23–4. Julius Stone refers to this as the ‘slot machine theory’ of legal reasoning, whereby inputs (‘P’) guarantee outputs (‘Q’): J. Stone, *Legal System and Lawyers’ Reasonings* (1964), at 235.

and accept the social institution accept they are true.¹⁰¹ For example, it is a brute fact of the world that two-thirds of the Earth's surface is covered in salt water, but an institutional fact that all parts of the sea not included in the territorial sea or exclusive economic zone count as the 'High Seas'. The institutional facts of the international law system (like the fact of the High Seas) are only facts because states and international lawyers accept that they are true; thus, some parts of the oceans *do* count as the High Seas, because those engaged in the practice of international law accept that this is the case. (note: this institutional fact is still a fact, and anyone who says there is no such thing as the High Seas is objectively, factually wrong).

Reasoning about the facts of the international law system takes place, then, within the context of the social practice of international law.¹⁰² When asked a question about international law, *I* can use deductive reasoning to give an answer, with the solution being implied by what *I* already know about the established rules and what *I* believe about the nature, structure and organizing principles of that system. But it is not enough for me alone (working in the 'I' mode) to reason that P implies Q, because the construction of knowledge in the international law system is a social process, undertaken collectively by those working within the framework provided by the social institution of international law.¹⁰³ *we*, collectively, as international lawyers, must reason that P implies Q, based on what *we* already know and what *we* believe. The *modus ponens* can, then, be reformulated in the following way in the case of deductive reasoning by international lawyers:

If (we, international lawyers, believe and understand that) P, then Q

P

Therefore (we, international lawyers, believe and understand that) Q.

Take our example concerning the deduction of the existence and content of rules of customary international law. 'I' can use deductive reasoning to explain the existence and content of a customary rule, based on what 'I' know about the established rules and what 'I' believe about the nature, structure and organizing principles of the international law system. But if my conclusion is inconsistent with what other international lawyers know and believe about the international law system, then 'I' cannot make the case that 'we', international lawyers, believe and understand some fact about the scope and content of customary international law. The necessary implication must be that my deductive conclusions cannot be characterized as being 'true' or 'false', only 'strong' or 'weak', depending on the extent to which they align with the knowledge and beliefs of other practitioners of international law – paradigmatically, the ICJ, which has the loudest voice in any debate on questions of international law.

There are, then, three steps in the process of deductive reasoning for me, as an international lawyer: first, I reflect on what I already know and believe about the content, nature, structure and organizing principles of the international law system; second, I rely on my knowledge and beliefs to reach a deductive conclusion, making explicit something implicit in what I already know and believe; finally, I test my deductive conclusion by considering whether other international lawyers

¹⁰¹On the difference between brute facts and institutional facts see, classically, G. E. M. Anscombe, 'On Brute Facts', (1958) 18(3) *Analysis* 69.

¹⁰²On the difference between the deductive logic of the syllogism and the deductive logic of the law see C. W. Jenks, *The Prospects of International Adjudication* (1964), at 646. The philosopher of science, Jerrold Aronson explains that:

Any type of system has its own set of laws, and its behavior is constrained by those laws. So what we deduce about the behavior of a given system . . . depends on what kind of a system it is . . . and the laws that govern the system.

J. L. Aronson, 'Mental Models and Deduction', (1997) 40(6) *American Behavioral Scientist* 782, at 792.

¹⁰³M. Koskeniemi, 'Methodology of International Law', (2007) *Max Planck Encyclopedia of Public International Law*, para. 1 ('International law is an argumentative practice . . . But it is the consensus in the profession . . . that determines, at any moment, whether a particular argument is or is not persuasive.')

– paradigmatically, the ICJ – would have reached the same conclusion, given their knowledge and beliefs, with any differences explained by different understandings about the content, nature, structure and organizing principles of the international law system.¹⁰⁴ In other words, to make a cogent claim concerning some alleged fact of international law, I must be able to reformulate my deductive conclusion in terms that, ‘We, international lawyers, believe and understand this fact to be true.’

4.2 Deduction of customary rules from existing custom

The existence of customary rules can be deduced from the existence of recognized and accepted rules of customary international law, which themselves reflect a general practice that is accepted as law.¹⁰⁵ In *Legal Consequences of the Construction of a Wall*, for example, the ICJ deduced the rule prohibiting the acquisition of territory using military force from the rule prohibiting the use of force:

The Court first recalls that [under] the United Nations Charter: “All Members shall refrain in their international relations from the threat or use of force” . . . On 24 October 1971, the General Assembly adopted [the Declaration on Friendly Relations], in which it emphasized that “No territorial acquisition resulting from the threat or use of force shall be recognized as legal.” As the Court stated in [its 1986 Nicaragua judgment], the principles as to the use of force incorporated in the Charter reflect customary international law . . . the same is true of its corollary entailing the illegality of territorial acquisition resulting from the threat or use of force.¹⁰⁶

It is important to note that the Court does not simply apply deductive (If P, then Q) logic, i.e., the ICJ does not simply claim that implicit in the customary rule prohibiting the use of force is the rule that states may not acquire territory using force. Instead, the Court frames the argument in terms of its more general understanding of the international law system, also pointing out that its deductive conclusion fits with that of states on the same issue, as reflected in the Friendly Relations Declaration.

4.3 Deduction of customary rules from sovereignty

Customary rules can also be deduced from the fundamental principles of the international law system.¹⁰⁷ The ICJ explains the point this way in *Delimitation of the Maritime Boundary in the Gulf of Maine Area*:

[Custom] comprises a limited set of norms for ensuring the co-existence and vital co-operation of the members of the international community, together with a set of

¹⁰⁴This understanding of deductive reasoning draws on the ‘mental model’ of deduction. See P. N. Johnson-Laird, ‘Mental Models and Probabilistic Thinking’, (1994) 50 *Cognition* 189, at 192:

[T]he underlying idea is that reasoning depends on constructing a model (or set of models) based on the premises and general knowledge, formulating a conclusion that is true in the model(s) and that makes explicit something only implicit in the premises, and then checking the validity of the conclusion by searching for alternative models of the premises in which it is false.

The mental model explains that we reason deductively by constructing a mental model, based on what we know and believe, in order to solve a certain problem. We use our model to reach a deductive conclusion which is implicit in what we know and believe to be the case. We then test our conclusion against the conclusions of others, using different models, based on different premises. See P. N. Johnson-Laird, ‘Mental Models and Deduction’, (2001) 5(10) *Trends in Cognitive Sciences* 434, at 435.

¹⁰⁵See, for example, *Pulp Mills on the River Uruguay (Argentina v. Uruguay)*, Judgment of 20 April 2010, [2010] ICJ Rep. 14, at 55–6, para. 101 (‘It is “every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States” . . . A State is thus obliged to use all the means at its disposal in order to avoid activities which take place in its territory . . . causing significant damage to the environment of another State.’).

¹⁰⁶*Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion of 9 July 2004, [2004] ICJ Rep. 136, at 171, para. 87.

¹⁰⁷See, for example, *Jurisdictional Immunities of the State (Germany v. Italy)*, Judgment of 3 February 2012, [2012] ICJ Rep. 99, at 123, para. 57 (‘[T]he rule of State immunity . . . derives from the principle of sovereign equality of States.’).

customary rules whose presence in the *opinio juris* of States can be tested by induction based on the analysis of a sufficiently extensive and convincing practice, and not by deduction from preconceived ideas.¹⁰⁸

Here, the ICJ divides customary rules into two types: those rules whose existence must be shown by an inductive methodology, by examining the evidence of state practice and *opinio juris*; and a limited set of essential customary rules whose existence can be shown by deduction from preconceived ideas. Whereas the inductive methodology starts with the collection of empirical evidence, deductive reasoning produces a novel conclusion from the existing knowledge and beliefs of international lawyers, without the need to collect new data in the form of state practice and *opinio juris*.¹⁰⁹

The case for the existence of essential customary rules identified by way of deduction is often framed in terms of the fundamental rights of states.¹¹⁰ State sovereignty is said to imply the existence of certain 'fundamental rights', which are logically and necessarily required to protect the sovereignty of the state.¹¹¹ Thus, a political community which counts as a sovereign state enjoys the fundamental rights of the sovereign state,¹¹² with those rights expressed in terms of regulative rules.

Ricardo J. Alfaro outlines the deductive argument for the existence of fundamental rights in the following way: an organized political community 'is a State because it is independent and sovereign'.¹¹³ Sovereignty and independence 'are consubstantial [i.e., of one and the same substance or essence] with the State and inseparable from it'.¹¹⁴ From this we can imply the existence of certain rights, which are inherent in the status of being a state. These are the fundamental rights 'without which it is impossible for the State to exist or for the mind to conceive it'.¹¹⁵ The alienation of these rights 'would mean the disappearance of the State[,] i.e., it would not be a State any more'.¹¹⁶ Alfaro gives the example of the non-intervention rule, explaining that: because the state is independent, 'it has the right to live free from external control and have its independence respected by other States'.¹¹⁷ If this were not the case, the political community would no longer be a state. The sovereignty and independence of the state logically and necessarily, then, implies the existence of 'the basic duty of non-intervention'.¹¹⁸

The non-intervention rule is the most widely cited example of a fundamental right of states,¹¹⁹ being expressly referenced in the key documents on fundamental rights.¹²⁰ When the rule came before the ICJ, the Court explained its understanding in the following way:

¹⁰⁸*Delimitation of the Maritime Boundary in the Gulf of Maine Area (Canada/United States of America)*, Judgment of 12 October 1984, [1984] ICJ Rep. 246, at 299, para. 111.

¹⁰⁹Tomuschat, *supra* note 59, at 299.

¹¹⁰W. G. Werner, 'State Sovereignty and International Legal Discourse', in I. F. Dekker and W. G. Werner (eds.), *Governance and International Legal Theory* (2004), 125, at 144.

¹¹¹Daniel Joyner explains that the adjective 'fundamental' is intended to make clear 'the link between states' rights and the sovereignty of states *per se*'. D. H. Joyner, 'Fundamental Rights of States in International Law and the Right to Peaceful Nuclear Energy', (2015) 4 *Cambridge Journal of International and Comparative Law* 661, at 664. See also H. P. Aust, 'Fundamental Rights of States: Constitutional Law in Disguise?', (2015) 4 *Cambridge International Law Journal* 521, at 525.

¹¹²See Oppenheim, *supra* note 71, at 158 ('[F]undamental rights are a matter of course, and self-evident, since the Family of Nations consists of Sovereign States.').

¹¹³R. J. Alfaro, 'The Rights and Duties of States', (1959) 97 *Recueil des Cours* 95, at 95.

¹¹⁴*Ibid.*, at 96.

¹¹⁵*Ibid.*, at 103.

¹¹⁶*Ibid.*, at 113.

¹¹⁷*Ibid.*, at 98.

¹¹⁸*Ibid.*, at 112.

¹¹⁹J. Crawford, *Brownlie's Principles of Public International Law* (2019), at 431.

¹²⁰See 1933 Montevideo Convention on the Rights and Duties of States, reprinted (1934) 28 (Supplement) AJIL 75, Art. 8; 1949 Draft Declaration on Rights and Duties of States, reprinted in General Assembly Res. 375(IV), Art. 3; General Assembly Res. 2625 (XXV), 1970 Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations.

The principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference; though examples of trespass against this principle are not infrequent, the Court considers that it is part and parcel of customary international law. [The principle of non-intervention] has moreover been presented as a corollary of the principle of the sovereign equality of States [in the Declaration on Friendly Relations, which set out the ‘basic principles’ of international law].¹²¹

There are four points to note here: first, non-intervention is tied to sovereignty; second, the ICJ appears unconcerned with the ‘not infrequent’ instances of inconsistent state practice; third, the ICJ references a deductive methodology when it notes that non-intervention has been ‘presented as a corollary of the principle of the sovereign equality of States’; finally, the ICJ aligns its deductive conclusions with the knowledge and beliefs of states, reflected in the Declaration on Friendly Relations.

5. A regulative rule of sovereignty

The previous sections showed that certain ‘fundamental rights’ of states can be deduced from the constitutive rule of sovereignty.¹²² Whilst we might look for evidence of state practice and *opinio juris*, this is not necessary to confirm the existence of these essential rules: the factual existence of the fundamental rights of states is understood to be logically and necessarily implied by the principle of state sovereignty.¹²³ The argument can be expressed as follows: some political communities count as sovereign states; this implies the existence of certain essential regulative rules to protect the ‘sovereignty’ of the state; these essential regulative rules are logically and necessarily required for international law to maintain its core identity as a legal system made by, and for, ‘sovereign’ states – i.e., without these essential regulative rules, the international law system would be a different kind of law system for different kinds of actors.

We see this kind of deductive reasoning in the Tallinn Manual 2.0. when it claims that ‘A number of principles and rules of conventional and customary international law derive from the general principle of sovereignty.’¹²⁴ The Manual further notes that ‘A well-accepted definition of “sovereignty” was set forth in the *Island of Palmas* award of 1928.’¹²⁵ In the award, Max Huber explains that sovereignty signifies the exclusive right of the state ‘to exercise [within a certain territory], to the exclusion of any other State, the functions of a State’.¹²⁶ This results in the following deductive claim:

If (we, international lawyers, believe and understand that) some political communities count as sovereign states, and sovereignty includes the exclusive right to exercise sovereign authority with respect to a territory, *then* it must be wrong for another state to exercise sovereign authority on that territory;

States are sovereign, and sovereignty does include the exclusive right to exercise sovereign authority with respect to a territory;

¹²¹See *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 9, at 106, para. 202.

¹²²S. M. Carbone and L. Schiano di Pepe, ‘States, Fundamental Rights and Duties’, (2009) *Max Planck Encyclopedia of Public International Law*, para. 1 (Fundamental rights are ‘rights and duties inherently linked to the creation and the essence itself of a State and, thus, independent of other sources of legal obligation of a voluntary or customary . . . character.’).

¹²³See Talmon, *supra* note 60, at 423 (customary rules can be ‘inferred from axiomatic principles such as sovereignty’).

¹²⁴See Tallinn Manual, *supra* note 15, Rule 1, Explanatory para. 3.

¹²⁵*Ibid.*, para. 2.

¹²⁶*Island of Palmas (Netherlands v. USA)*, Award of 4 April 1928, 2 RIAA 829 (1928), at 838.

Therefore (we, international lawyers, believe and understand that), it must be wrong – as a matter of international law – for one state to exercise sovereign authority on the territory of another state (without consent or a permissive rule of international law).

The veracity of this logically valid output depends on accepting Huber's definition as *the* correct definition of 'sovereignty'. Whilst some are not convinced,¹²⁷ most international lawyers who have written on sovereignty have relied on Huber's understanding.¹²⁸ James Crawford, for example, contends that 'sovereignty involves a monopoly of governing authority', making direct reference to the *Island of Palmas* award.¹²⁹ The argument for the regulative rule of sovereignty is, then, both logically valid and based on a sound premise.

The remaining question is whether the deductive claim for the existence of the regulative rule of sovereignty aligns with the knowledge and beliefs of other international lawyers, paradigmatically the ICJ. In *Corfu Channel*, the ICJ made the point that 'Between independent States, respect for territorial sovereignty is an essential foundation of international relations.'¹³⁰ In its 1986 *Nicaragua* (Merits) judgment, the ICJ determined that unauthorized overflights by government aircraft were 'in breach of [the United States'] obligation under customary international law not to violate the sovereignty of another State'¹³¹ The ICJ's understanding of the content, nature, structure and organizing principles of the international law system provides support, then, for the deductive conclusion that a regulative rule of sovereignty is logically and necessarily required to protect the sovereignty of the state.

The deductive logic of international law confirms the existence of a regulative rule of sovereignty, which is logically and necessarily implied by the constitutive rule of sovereignty: political communities which count as states (the constitutive rule of sovereignty) must not violate the sovereignty of other states (the regulative rule of sovereignty). The regulative rule applies – like all general international law rules – in the physical domain and in the cyber domain.¹³² Thus, we can conclude that the United Kingdom and United States are factually wrong when they deny the existence of a regulative rule of sovereignty as a matter of existing international law (*lex lata*). The real question, to which this article now turns, is this: what is the content of the regulative rule of sovereignty?

6. Content of the regulative rule of sovereignty

Ordinarily, the identification of the existence and content of a customary rule takes place at the same moment, with both the existence and content being manifested in the evidence of state

¹²⁷Vaughn Lowe, for example, complains that whilst Huber's formula provides a framework for addressing the question of who the Sovereign is, 'it is of much less help when the question is whether that sovereignty has or has not been infringed by the acts of another State': V. Lowe, 'Customary Principle of Sovereignty of States in the Nicaragua Case', in E. Sobenes Obregon and B. Samson (eds.), *Nicaragua Before the International Court of Justice* (2017), 269, at 270.

¹²⁸T. E. Aalberts, *Constructing Sovereignty Between Politics and Law* (2012), at 56 ('Within legal discourse, an authoritative definition of sovereignty is provided in the *Island of Palmas* case.'). See, for example, S. Besson, 'Sovereignty', (2011) *Max Planck Encyclopedia of Public International Law*, para. 56; J. C. Cooper, 'High Altitude Flight and National Sovereignty', (1951) 4 *International Law Quarterly* 411, at 411; T. M. Franck, 'Multiple Tiers of Sovereignty', (1994) 88 *Proceedings of the American Society of International Law* 51, at 51; N. Schrijver, 'The Changing Nature of State Sovereignty', (1999) 70 *British Yearbook of International Law* 65, at 70; M. N. Shaw, 'The International Court of Justice and the Law of Territory', in C. J. Tams and J. Sloan (eds.), *The Development of International Law by the International Court of Justice* (2013), 151, at 152.

¹²⁹See Crawford, *supra* note 30, at 120–1.

¹³⁰See *Corfu Channel case*, *supra* note 43, at 35.

¹³¹See *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 9, at 128, para. 251 and at 147, Operative paragraph (5).

¹³²Akande et al., *supra* note 18, at 35.

practice and *opinio juris*.¹³³ We have already seen, in relation to the rule of sovereignty, that there is limited state practice in the physical domain and no clear state practice in the cyber domain to allow us to identify the content of the rule. There is, furthermore, no consensus in the *opinio juris*: there are those states who have expressed a belief in the existence of the rule of sovereignty, but without taking a position on its content – Austria,¹³⁴ Bolivia,¹³⁵ Chile,¹³⁶ and Estonia;¹³⁷ states who consider that the rule of sovereignty prohibits any state cyber operation targeting the ICTs in another state – China,¹³⁸ Finland,¹³⁹ France,¹⁴⁰ Guatemala,¹⁴¹ and Iran;¹⁴² other states who argue that the rule of sovereignty only prohibits state cyber operations resulting in damage or a loss of functionality to the ICTs in another state – Canada,¹⁴³ Czech Republic,¹⁴⁴ Germany,¹⁴⁵ Italy,¹⁴⁶ New Zealand,¹⁴⁷ and Sweden;¹⁴⁸ and, finally, states who consider that the rule of sovereignty specifically prohibits state cyber operations targeting ICTs used for inherently governmental functions – Czech Republic,¹⁴⁹ Finland,¹⁵⁰ Guyana,¹⁵¹ The Netherlands,¹⁵² New Zealand,¹⁵³ Sweden,¹⁵⁴ and Switzerland,¹⁵⁵ including ICTs used in elections – Canada,¹⁵⁶ and Germany.¹⁵⁷

The content of customary rules can sometimes be identified by way of deduction. We see this, for example, in the ICJ's judgment in *Arrest Warrant of 11 April 2000*. The Court began by confirming the existence of the customary rule providing that Ministers for Foreign Affairs enjoy immunity from the criminal jurisdiction of other states.¹⁵⁸ The relevant question was whether the content of the rule recognized an exception in cases concerning accusations of crimes against humanity. To answer this, the ICJ made the following deductive argument: the purpose of the customary rule is to ensure that foreign ministers can effectively carry out their functions on behalf of their states; in the performance of these functions, they are often required to travel internationally; this logically requires that, throughout the terms of their office, when abroad, foreign ministers must enjoy full immunity from the jurisdiction of the courts of other states. Therefore,

¹³³See Talmon, *supra* note 60, at 418 ('The determination of a [customary] rule and that of its content and scope are frequently one and the same.').

¹³⁴See Austria, *supra* note 78.

¹³⁵See Hollis Fourth Report, *supra* note 76.

¹³⁶See *ibid.*

¹³⁷See Estonia, *supra* note 83.

¹³⁸See China, *supra* note 84, at 2.

¹³⁹See Finland, *supra* note 85, at 2.

¹⁴⁰See France, *supra* note 86, at 3.

¹⁴¹See Hollis Fourth Report, *supra* note 76.

¹⁴²See Iran, *supra* note 90, Art. II(3).

¹⁴³See Canada, *supra* note 80, para. 15.

¹⁴⁴See Czech Republic, *supra* note 82.

¹⁴⁵See Germany, *supra* note 87, at 4.

¹⁴⁶See Italy, *supra* note 91, at 4.

¹⁴⁷See New Zealand, *supra* note 93, para. 14.

¹⁴⁸See Sweden, *supra* note 94, at 2.

¹⁴⁹See Czech Republic, *supra* note 82.

¹⁵⁰See Finland, *supra* note 85, at 2.

¹⁵¹See Hollis Fourth Report, *supra* note 76.

¹⁵²See The Netherlands, *supra* note 92, at 3.

¹⁵³See New Zealand, *supra* note 93, para. 11.

¹⁵⁴See Sweden, *supra* note 94, at 2.

¹⁵⁵See Switzerland, *supra* note 95, at 3.

¹⁵⁶Canada argues that cyber operations producing significant harmful effects on the exercise of governmental functions are wrongful, including those targeting '[the] administration of elections': See Canada, *supra* note 80, para. 18.

¹⁵⁷Germany maintains that 'Foreign interference in the conduct of elections of a State may under certain circumstances constitute a breach of sovereignty': See Germany, *supra* note 87, at 3.

¹⁵⁸*Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, Judgment of 14 February 2002, [2002] ICJ Rep. 3, at 20–1, para. 51.

the issuing of an arrest warrant for a serving Minister for Foreign Affairs infringed the immunity from criminal jurisdiction enjoyed by them under international law.¹⁵⁹

The Tallinn Manual 2.0. deploys deductive reasoning to explain the content of the cyber rule of sovereignty. The Manual is central to these discussions because it has set the terms of the debate,¹⁶⁰ with all scholars,¹⁶¹ and several states,¹⁶² explaining their positions by reference to the Tallinn Manual. The Manual deduces the content of the regulative rule of sovereignty from Max Huber's definition of sovereignty in the *Island of Palmas* award: '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.'¹⁶³

From this formulation of sovereignty, the Tallinn Manual deduces the content of the cyber rule of sovereignty: first, states must not conduct cyber operations that target the cyber infrastructure located on the territory of another state; second, states must not conduct cyber operations targeting the inherently governmental functions of another state.¹⁶⁴ The argument can be formulated as follows:

If the correct definition of sovereignty was given by Max Huber, then the rule of sovereignty prohibits state activities on the territory of another state and state activities targeting the inherently governmental functions of another state;

*We do believe and understand that the correct definition was given in the *Island of Palmas* award;*

Therefore, the rule of sovereignty prohibits state activities on the territory of another state and state activities targeting the inherently governmental functions of another state.

This is a logically valid argument, built on a sound premise, i.e., Huber's definition captures the essence of state sovereignty (see above). The main question, then, is as follows: are the Tallinn Manual's deductive conclusions on the content of the cyber rule of sovereignty aligned with the knowledge and beliefs of other international lawyers, thereby reflecting a shared understanding of the content, nature, structure and organizing principles of the international law system?

6.1 Prohibition on targeting cyber infrastructure in another state

The group of experts responsible for drafting the Tallinn Manual were agreed that the rule of sovereignty prohibits *in situ* state cyber operations by state agents physically present on the territory of the target state (e.g., inserting a USB flash drive to introduce malware). The deductive argument for this position is explained as follows: (i) a number of customary rules derive from

¹⁵⁹*Ibid.*, para. 71. The judgment was subject to critical comment, showing that valid deductive conclusions, based on agreed premises, are not always accepted by other international lawyers. See, for example, A. Cassese, 'When May Senior State Officials Be Tried for International Crimes? Some Comments on the Congo v Belgium Case', (2002) 13 EJIL 853.

¹⁶⁰See Efrony and Shany, *supra* note 68, at 584–5.

¹⁶¹See, as just one example, K. E. Eichensehr, 'Not Illegal: The SolarWinds Incident and International Law', (2022) *European Journal of International Law*, Virginia Public Law and Legal Theory Research Paper No. 2022-53 (SSRN), at 10 ('The Tallinn Manual suggests that a sovereignty violation can occur via a breach of a state's territorial integrity or an "interference with or usurpation of inherently governmental functions".').

¹⁶²See, for example, express reference to the Tallinn Manual in the positions of Canada, *supra* note 80, para. 15; Finland, *supra* note 85, at 2; Germany, *supra* note 87, at 3–4; Sweden, *supra* note 94, at 2.

¹⁶³See *Island of Palmas*, *supra* note 126, at 838.

¹⁶⁴See Tallinn Manual, *supra* note note 15, Rule 4, Explanatory para. 10.

(The precise legal character of remote cyber operations that manifest on a state's territory is somewhat unsettled in international law. The International Group of Experts assessed their lawfulness on two different bases: (1) the degree of infringement upon the target State's territorial integrity; and (2) whether there has been an interference with or usurpation of inherently governmental functions).

the principle of sovereignty; (ii) this includes the regulative rule of sovereignty; (iii) sovereignty signifies the exclusive right of the state to exercise, within a certain territory, the functions of a state; (iv) based on its internal sovereignty, a state may control access to its territory; (v) there is a violation of the rule of sovereignty whenever one state physically crosses into the territory of another state without its consent;¹⁶⁵ (vi) *therefore*, any non-consensual state cyber activities on the territory of another state violate the regulative rule of sovereignty.¹⁶⁶

One problem is that the Tallinn Manual appears to be conflating two regulative rules here: the rule that says, ‘Do not enter the territory of another State without its consent’, and the rule that says, ‘Do not carry out any activities on the territory of another State, without its consent.’ Moreover, the Tallinn Manual appears to be deducing the second rule from the first, whereas the most obvious deductive claim is that the exclusive right of the state to exercise, within a certain territory, the functions of a state logically and necessarily precludes the exercise of sovereign authority by another state on that territory. Notwithstanding the deficiencies in logic, the Tallinn Manual’s deductive conclusion – that the exercise of governmental power on the territory of another state is a violation of the rule of sovereignty – is supported by the conclusions of the ICJ. In *Certain Activities/ Construction of a Road*, for example, Costa Rica alleged that Nicaragua had violated its territorial sovereignty in the area of Isla Portillos by excavating a channel (‘caño’), with the aim of connecting the San Juan River with the Harbor Head Lagoon. Nicaragua did not contest the facts but maintained that it had full sovereignty over the caño. The ICJ disagreed, concluding that the disputed territory belonged to Costa Rica. Consequently, Nicaragua’s dredging activities on Costa Rican territory, ‘were in breach of Costa Rica’s territorial sovereignty’.¹⁶⁷

The cyber rule of sovereignty prohibits, then, state cyber operations from being conducted on the territory of another state, for the reason that the regulative rule of sovereignty prohibits states from carrying out non-consensual activities on the territory of another state, i.e., whilst state agents are physically present on the territory of the other state. This is one of the essential rules of customary international law, logically deduced from the principle of sovereignty. A good example of a violation of this rule would be the efforts of the Russian GRU intelligence cyber warfare team, in 2018, to carry out a closed access hack operation targeting the Wi-Fi network of the Organisation for the Prevention of Chemical Weapons in the Hague – on the territory of the Netherlands.¹⁶⁸

The Tallinn Manual then makes another deductive step: because a state controls access to its territory, there is a violation of the rule of sovereignty when a remote, *ex situ* state cyber operation targets the cyber infrastructure located in another state. The Manual is clear that this regulative rule ‘is based on the premise that a State controls access to its sovereign territory’.¹⁶⁹ The argument finds some support in the literature,¹⁷⁰ and in the views of some states. Finland, for example, explains the logic of the position in the following way (although note the equivocation in the final sentence):

The International Court of Justice has consistently confirmed that it is a duty of every State to respect the territorial sovereignty of others. This applies to unauthorized intrusions to physical spaces such as overflight of a State’s territory by an aircraft belonging to another State . . . Similarly, a non-consensual intrusion in the computer networks and systems that rely on the

¹⁶⁵*Ibid.*, para. 10 (this regulative rule ‘is based on the premise that a State controls access to its sovereign territory’).

¹⁶⁶*Ibid.*, para. 6.

¹⁶⁷*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)*, Merits, Judgment of 16 December 2015, [2015] ICJ Rep. 665, at 703, para. 93.

¹⁶⁸How the Dutch foiled Russian “cyber-attack” on OPCW, *BBC News*, 4 October 2018.

¹⁶⁹See Tallinn Manual, *supra* note 15, Rule 4, Explanatory para. 10.

¹⁷⁰See, for example, W. Heintschel von Heinegg, ‘Territorial Sovereignty and Neutrality in Cyberspace’, (2013) 89 *International Law Studies* 123, at 124.

cyber infrastructure in another State's territory *may* amount to a violation of that State's sovereignty.¹⁷¹

The deductive argument for the Tallinn Manual's rule prohibiting remote state cyber operations targeting the ICTs in another state proceeds as follows: (i) a number of customary rules derive from the principle of sovereignty; (ii) this includes the regulative rule of sovereignty; (iii) sovereignty signifies the exclusive right of the state to exercise, within a certain territory, the functions of a state; (iv) based on its internal sovereignty, a state may control access to its territory; (v) this rule already applies to the state's officials and goods;¹⁷² (vi) by analogy, the rule also applies to malware,¹⁷³ software designed to cause damage or disruption, 'sent across' the state border, via the Internet;¹⁷⁴ (vii) therefore, remote state cyber operations targeting the ICTs in another state constitute a violation of the regulative rule of sovereignty.

But herein lies the problem: proponents of the rule of sovereignty cannot agree whether the rule prohibits all remote state cyber operations (the 'pure sovereignty' position), or only those resulting in damage or loss of functionality to ICTs (the 'relative sovereignty' position).¹⁷⁵ Moreover, neither argument works as a matter of international law deductive reasoning, meaning that no general prohibition on remote state cyber operations can be deduced from the sovereignty of the target state.

The relative sovereignty position does not work as a matter of deductive logic. It contends that remote state cyber operations violate the rule of sovereignty *only* when they cause damage or loss of functionality to ICTs. This is the dominant position amongst proponents of the cyber rule of sovereignty.¹⁷⁶ The argument can be expressed as follows: *if* the sovereignty of the state accords the state the right to control access to its territory, *then* there is a violation of the rule of sovereignty whenever malware 'sent across' the border by a state causes damage or loss of functionality to ICTs on the territory of the target state. But this argument does not work: *if* we accept that the wrongful act is the crossing of the state border without consent,¹⁷⁷ *then* it cannot logically be the case that only some remote cyber operations are prohibited. We cannot deduce the requirement for evidence of damage or loss of functionality from the right of the state to control access to its territory, for the reason that we cannot explain why there is no violation when malware 'sent across' the border fails to cause damage or loss of functionality to ICTs – as with the case of 'backdoors', malware which allows for later access by outside powers (e.g., the SolarWinds hack, whereby Russia accessed US federal government computers, without causing damage or loss of functionality).¹⁷⁸

¹⁷¹See Finland, *supra* note 85, at 2 (emphasis added).

¹⁷²In *Right of Passage over Indian Territory*, the ICJ confirmed that the territory state has the right to determine whether, or not, officials and goods from another state can enter its territory: *Right of Passage over Indian Territory (Portugal v. India)*, Merits, Judgment 12 April 1960, [1960] ICJ Rep. 6, at 40. The fact that state officials and goods have no right of entry does not logically mean there is a violation of international law if they enter the territory without permission; it simply means that the state has no right to complain if its officials or goods are denied entry.

¹⁷³Whilst the analogy between malware and physical persons and goods is not self-evident, it does have merit. Consider, for example, the different ways that a state could destroy a nuclear facility: by sending human troops across the border; by firing a physical missile targeting the facility; or, by way of targeted malware (e.g., Israel's Stuxnet malware that destroyed Iranian nuclear facilities). On Stuxnet and the use for force see R. Buchan, 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', (2012) 17 *Journal of Conflict & Security Law* 211, at 219–21.

¹⁷⁴Whatever the technical details, most scholars and regulators think of the Internet as an 'end-to-end' communication system, ignoring the pathways that data packages flow through. See, for example, L. Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (2002), at 39–40.

¹⁷⁵On this distinction see H. Moynihan, *The Application of International Law to State Cyberattacks Sovereignty and Non-intervention* (2019), at 20, 24.

¹⁷⁶Schmitt, *supra* note 14, at 752 ('Consensus also appears to have coalesced around treating a relatively permanent loss of cyberinfrastructure functionality as the requisite damage.')

¹⁷⁷The Tallinn Manual is clear that the rule prohibiting remote state cyber operations 'is based on the premise that a State controls access to its sovereign territory': See Tallinn Manual, *supra* note 15, Rule 4, Explanatory para. 10.

¹⁷⁸See Eichensehr, *supra* note 161, at 10.

The approach of the pure sovereigntists, by way of contrast, is logically sound, but their conclusion is not shared by other international lawyers. The argument is straightforward: *if* the sovereignty of the state accords the state the right to control access to its territory, *then* there is a violation of the rule of sovereignty whenever another state's malware crosses into the territory without consent. All remote state cyber operations, even those causing no damage or loss of functionality (e.g., installing backdoors for later entry), are, on this understanding, violations of the rule of sovereignty. Some states, notably China¹⁷⁹ and France,¹⁸⁰ and some authors,¹⁸¹ including some of the experts responsible for the Tallinn Manual, adopt this catch-all position. However, most states and most scholars, including most proponents of the cyber rule of sovereignty,¹⁸² and most of those responsible for the Tallinn Manual,¹⁸³ do not accept this conclusion. The point is significant, because, whilst the process of deductive reasoning involves reflecting on what we already know and believe to draw a novel conclusion, the outcome is only argumentatively forcible when accepted by other international lawyers, with any disagreement explained by different understandings of international law. Given that most states and most academics do not agree that the sovereignty of the state logically and necessarily implies a prohibition on all remote state cyber operations, we must conclude that the pure sovereigntists have a different understanding of the nature, structure and organizing principles of the international law system to that possessed by most states and international lawyers. The result is that the pure sovereigntists cannot reframe their deductive claims in the required form that 'We, international lawyers, believe and understand that all remote State cyber operations violate the rule of sovereignty.'

6.2 Prohibition on targeting governmental functions

The Tallinn Manual's international experts further concluded that the rule of sovereignty prohibits cyber operations that interfere with, or usurp, the inherently governmental functions of another state. Again, the regulative rule is deduced from the nature of sovereignty, as defined in *Island of Palmas*. Two issues must be disaggregated: the claim that the rule of sovereignty prohibits remote cyber operations that *usurp* inherently governmental functions; and the claim that the rule prohibits cyber operations that *interfere* with the inherently governmental functions of another state.

6.2.1 Prohibition on usurping governmental functions

The Tallinn Manual's argument that the rule of sovereignty prohibits remote cyber operations which *usurp* the inherently governmental functions of the target state can be explained as follows: (i) a number of regulative rules derive from the principle of sovereignty; (ii) this includes the rule that a state must not conduct cyber operations that violate the sovereignty of another state; (iii) sovereignty was defined by Max Huber as the exclusive right of the state to exercise, within a certain territory, the functions of a state; (iv) therefore, the regulative rule of sovereignty prohibits state cyber operations which *usurp* (i.e., wrongfully appropriate) the inherently

¹⁷⁹See China, *supra* note 84, at 2 ('No State shall . . . access the ICT infrastructure of another State or infringe on the network systems within the jurisdiction of another State.').

¹⁸⁰See France, *supra* note 86, at 3 ('Any cyberattack against French digital systems . . . constitutes a breach of sovereignty.').

¹⁸¹See, for example, R. Buchan, *Cyber Espionage and International Law* (2018), at 51 ('Any non-consensual incursion by one state into the territory of another state violates the rule of territorial sovereignty, regardless of whether that infraction produces damage.').

¹⁸²See Schmitt, *supra* note 14.

¹⁸³Some of the experts responsible for the Tallinn Manual also argued for this understanding, pointing out that it is 'consistent with the object and purpose of the principle of sovereignty that affords States the full control over access to and activities on their territory'. But 'no consensus could be achieved [among the group of experts] 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'. See Tallinn Manual, *supra* note 15, Rule 4, Explanatory para. 14.

governmental functions of another State, 'because the target State enjoys the exclusive right to perform them, or to decide upon their performance'.¹⁸⁴

This is a valid deductive argument based on sound premises, accepted by most international lawyers:

If the correct definition of sovereignty was given by Max Huber, then the rule of sovereignty prohibits other states from wrongfully appropriating the sovereign powers of the state within its territory;

*We do believe and understand that the correct definition was given in *Island of Palmas*;*

Therefore, the rule of sovereignty prohibits state activities that usurp the inherently governmental functions of the state.

Support for this conclusion can be found in the judgment of the ICJ in *Certain Activities/Construction of a Road*. Nicaragua alleged that Costa Rica's construction works had resulted in sediment deltas on its territory, and that these constituted 'physical invasions, incursions by Costa Rica into Nicaragua's sovereign territory . . . through the agency of sediment'. This, it was claimed, amounted to a 'trespass', meaning that Costa Rica had 'violated Nicaragua's territorial integrity and sovereignty'.¹⁸⁵ The ICJ rejected the claim, concluding that the argument for a violation of territorial integrity 'via sediment [was] unconvincing'. The ICJ also noted that there was 'no evidence that Costa Rica exercised any authority on Nicaragua's territory or carried out any activity therein . . . Therefore, Nicaragua's claim concerning the violation of its territorial integrity and sovereignty must be dismissed'.¹⁸⁶

A reverse reading of the judgment strongly suggests the opposite: the exercise of state authority in the territory of another state (as well as any governmental activity carried out by state agents *therein*, i.e., whilst physically present on the territory) is a violation of the rule of sovereignty, since the territorial state has the exclusive right to exercise, within its territory, the functions of a state.

Remote state cyber operations involving the exercise of inherently governmental functions in the territory of another state violate the rule of sovereignty because only the territorial state has the right to exercise the functions of the state in its territory. One example would be a remote state cyber law enforcement operation, such as evidence gathering by hacking computers in another state (without permission or a permissive rule of international law),¹⁸⁷ because only the territorial state has the right to carry out criminal justice investigations in its territory (or to allow other actors to carry them out).¹⁸⁸ Inherently governmental functions like this must be distinguished from other state activities which do not implicate the rule of sovereignty.¹⁸⁹ Recall that, following *Island of Palmas*, sovereignty signifies the exclusive right of the state to exercise the functions of the state within a certain territory. This logically and necessarily excludes the possibility of other states exercising the functions of the state in the territory. But it does not logically and necessarily preclude the possibility of other remote state activities impacting the ICTs in the target state, i.e.,

¹⁸⁴*Ibid.*, para. 15.

¹⁸⁵See *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)*, *supra* note 167, at 77, para. 221.

¹⁸⁶*Ibid.*, para. 223 (emphasis added).

¹⁸⁷See Tallinn Manual, *supra* note 15, Rule 4, Explanatory para. 18.

¹⁸⁸H. Kelsen, 'Draft Declaration on Rights and Duties of States, The: Critical Remarks', (1950) 44 *American Journal of International Law* 259, at 267–8 ('If a state in the territory of another state performs, without the latter's consent, an act of jurisdiction[,] for instance, an act of investigation, it violates its duty to respect the territorial integrity of the other state.').

¹⁸⁹See, on this point, M. N. Schmitt, 'Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention', (2020) 96 *International Law Studies* 549, at 557 ('An inherently governmental function may best be understood as a function that States alone have the authority to perform (or authorize other entities to perform on their behalf). Classic examples include collecting taxes, conducting elections, and enforcing laws.')

activities which do not concern inherently governmental functions. Thus, for example, remote state ransomware operations, such as the WannaCry and NotPetya attacks, blamed respectively on North Korea and Russia,¹⁹⁰ are not concerned with the exercise of inherently governmental functions, and do not therefore implicate this aspect of the cyber rule of sovereignty.

6.2.2 Prohibition on interfering with governmental functions

The Tallinn Manual further claims that the rule of sovereignty prohibits remote cyber operations that *interfere* with inherently governmental functions. This is the aspect of the rule most relevant to election hacking.¹⁹¹ The conduct of elections is clearly an inherently governmental function. Malicious remote state cyber operations, such as DDoS attacks on the websites of political parties, the removal of voters from the electoral roll, or changing the outcome by hacking the vote tabulation software, constitute interferences with that inherently governmental function. A rule of sovereignty prohibiting interferences in the ICTs used in elections would, therefore, make unlawful all cases of election hacking.

The Tallinn Manual's deductive argument for the regulative rule prohibiting interferences in inherently governmental functions as one element of the cyber rule of sovereignty proceeds as follows: (i) a number of regulative rules derive from the principle of sovereignty; (ii) This includes the rule that a state must not conduct cyber operations that violate the sovereignty of another state; (iii) sovereignty concerns the exclusive right of the state to exercise, within a certain territory, the functions of a state; (iv) the rule of sovereignty, therefore, prohibits cyber operations that *interfere* with the inherently governmental functions of the target state, 'because the target State enjoys the exclusive right to perform them, or to decide upon their performance'.¹⁹² The deductive logic can be expressed in the following way:

If the correct definition of sovereignty was given by Max Huber, then the rule of sovereignty prohibits other states from interfering with the sovereign powers of the state;

*We do believe and understand that the correct definition was given in *Island of Palmas*;*

Therefore, the rule of sovereignty prohibits state activities that interfere with the inherently governmental functions of the territorial state.

This is a valid deductive argument, based on a sound premise accepted by most international lawyers: there are no errors in the application of the rules of logic; and sovereignty, as explained by Max Huber in *Island of Palmas*, does concern the right of the state 'to exercise [in regard to a portion of the globe], to the exclusion of any other State, the functions of a State'.¹⁹³

The difficulty lies with the Tallinn Manual's conclusion that the constitutive rule of sovereignty implies a 'non-interference' rule, since this reflects a different understanding of the nature, structure and organizing principles of the international law system to that held by most international lawyers.

The argument that the rule of sovereignty prohibits all remote state cyber operations that interfere with the inherently governmental functions of the target state can be explained as follows: some political communities count as sovereign states (the constitutive rule of sovereignty); the sovereignty of the state is consubstantial with state independence; this logically and necessarily implies the existence of a regulative rule that no state has the right to *interfere* in the government of another because this would negate the sovereignty of the target state.

¹⁹⁰These were not characterized by the victim states as violations of sovereignty: See Efrony and Shany, *supra* note 68, at 641. Domestic criminal laws may well apply to the individual state agents and the state organs responsible, and other rules of international law might apply to the state responsible.

¹⁹¹Schmitt, *supra* note 14, at 753 ('The issue in the election context is interference.').

¹⁹²See Tallinn Manual, *supra* note 15, Rule 4, Explanatory para. 15.

¹⁹³See *Island of Palmas*, *supra* note 126, 838.

The problem is that the non-intervention rule can be deduced in the same way: some political communities count as sovereign states; The sovereignty of the state is consubstantial with state independence; this logically and necessarily implies the existence of a regulative rule that no state has the right to *intervene* in the government of another because that would negate the sovereignty of the target state.¹⁹⁴ The key point is that there are two component elements in the non-intervention rule: interference *and* the use of methods of coercion. In the words of the ICJ, ‘The element of coercion . . . defines, and indeed forms the very essence of, prohibited intervention.’¹⁹⁵ States can interfere in the affairs of another state (unless the behaviour is covered by a specific regulative rule),¹⁹⁶ but they cannot interfere using coercive methods intended to compel the target state to take a course of action that it would not otherwise voluntarily pursue, since this would negate the sovereignty of the target state.

The process of deductive reasoning by international lawyers involves reflecting on what we already know and believe; and then drawing a novel conclusion, making explicit something implicit in what we already know and believe about international law. The outcome depends on the underlying knowledge and beliefs. The same knowledge and beliefs about international law cannot logically imply inconsistent outcomes. The point is significant. The existence of the non-intervention rule is implied by what we already know and believe about international law. There are two component elements, ‘interference’ *and* ‘coercion’.¹⁹⁷ The same knowledge and beliefs about international law cannot, logically, imply the non-interference rule, with its one component element of ‘interference’. To believe in the non-interference rule means not believing in the non-intervention rule, because the non-interference rule would effectively replace the non-intervention rule, since, as Michael Schmitt explains, in the case of the non-interference rule, ‘[t]here is no requirement that the interference be coercive, as is the case with intervention’.¹⁹⁸ Given that all international lawyers believe in the non-intervention rule, a non-interference rule cannot be logically and necessarily implied by what we already know and believe about the content, nature, structure and organizing principles of the international law system.

7. Conclusion

The rule of sovereignty has taken centre stage in the debates on the legal framework for responsible state behaviour in cyberspace, often generating more heat than light as states and scholars dispute whether sovereignty is a ‘rule’ or merely a ‘principle’. This article has considered the extent to which the rule of sovereignty can regulate malicious state cyber operations targeting the ICTs used in elections by highlighting the distinction between regulative and constitutive rules, because the rule of sovereignty can be expressed in terms that: a political community which counts as a state (the constitutive rule of sovereignty) must not violate the sovereignty of another state (the regulative rule of sovereignty). Framing the discussion this way allowed us to evaluate the strengths of the claims for the identification of the existence and content of the regulative rule of sovereignty in the cyber domain, leading to the following conclusions.

¹⁹⁴For an early example of the argument that the non-intervention rule is implied by the ‘sovereignty’ of the state, see E. de Vattel, *The Law of Nations, Or, Principles of the Law of Nature, Applied to the Conduct and Affairs of Nations and Sovereigns* [1797] (2008), Book II, Chapter IV, para. 54.

¹⁹⁵See *Military and Paramilitary Activities in and against Nicaragua*, *supra* note 9, para. 205.

¹⁹⁶E.g., the prohibition on subversive propaganda. See, for example, J. B. Whitton, ‘Propaganda and International Law’, (1948) 72 *Recueil des Cours* 542, at 582–3.

¹⁹⁷The prohibition is on coercive interference – and not interference *per se*: M. Jamnejad and M. Wood, ‘The Principle of Non-intervention’, (2009) 22 *Leiden Journal of International Law* 345, at 348. Coercion, or its functional equivalent, such as dictatorial interference, has been a component element in the non-intervention principle at least since the end of the nineteenth century. See, classically, Oppenheim, *supra* note 71, at 181–2.

¹⁹⁸See Schmitt, *supra* note 14, at 753.

First, a regulative rule of sovereignty can be deduced from the constitutive rule of sovereignty. This regulative rule is logically and necessarily required for international law to maintain its identity as a legal system made by, and for, sovereign states. In other words, if international law did not protect the 'sovereignty' of those political communities which count as states, it would not be the international law system that we know and understand.

Secondly, the content of the regulative rule of sovereignty can be deduced from the nature of sovereignty. Whilst imperfect and inelegant, the definition provided by Max Huber in *Island of Palmas* captures the essence of how international lawyers understand the notion: sovereignty concerns the exclusive right of the state to exercise, within a certain territory, the functions of a state. Thus, in *Case of the SS 'Lotus'*, the Permanent Court of International Justice confirmed that '[T]he first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State.'¹⁹⁹

Thirdly, the essential regulative rule of sovereignty prohibits state agents from carrying out non-consensual activities on the territory of another state. *In situ* state cyber operations carried out on the territory of another state are violations of the rule of sovereignty.

Fourthly, the rule of sovereignty does not prohibit all remote, *ex situ* state cyber operations targeting ICTs located in another state. Neither of the deductive claims for a regulative rule based on the wrong of malware entering the territory without consent works: the relative sovereignty position cannot explain why the violation of a rule based on the wrong of non-consensual entry logically requires evidence of damage or loss of functionality to ICTs; whereas, the deductive conclusion of the pure sovereigntist position, that all remote state cyber operations violate the rule of sovereignty, is not shared by most states or international lawyers, including most proponents of the cyber rule of sovereignty.

Fifthly, the rule of sovereignty prohibits remote state cyber operations that usurp the inherently governmental functions of the target state. Sovereignty involves the exclusive right of the state to exercise, within the territory, the functions of a state. The exercise of sovereign authority in the territory of another state (without consent, or some permissive rule of international law) is a violation of the rule of sovereignty. Thus, state cyber operations involving the exercise of inherently governmental functions, such as remote law enforcement evidence gathering operations, are violations of the rule of sovereignty.

Finally, the rule of sovereignty does not prohibit remote state cyber operations that merely interfere with the exercise of governmental functions. To believe in the existence of the non-interference rule, as one element of the rule of sovereignty, means not believing in the non-intervention rule – and all states and all international lawyers, including the proponents of the rule of sovereignty, believe in the non-intervention rule. The answer to the problem of election interference, including election hacking, does not lie in the rule of sovereignty, but in exploring the meaning of 'coercion' in the non-intervention rule. As I have argued elsewhere, there are ways of understanding coercion that capture remote state cyber operations that take control of, or disable, the ICTs used in elections. This is coercive because the outside power by-passes the governmental institutions of the state, to ensure that the target state acts (or does not act) as intended by the outside power.²⁰⁰ Simply put: the solution to the problem of election hacking lies in a proper understanding of the recognized and accepted non-intervention rule, not in the contested and contestable rule of sovereignty.²⁰¹

¹⁹⁹SS *Lotus case (France v. Turkey)*, PCIJ Rep Series A No 10, at 18.

²⁰⁰See S. Wheatley, 'Foreign Interference in Elections under the Non-Intervention Principle: We Need to Talk about "Coercion"', (2020) 31 *Duke Journal of Comparative & International Law* 161, at 197.

²⁰¹S. Wheatley, 'Cyber and Influence Operations Targeting Elections: Back to the Principle of Non-Intervention', *EJIL: Talk!*, 26 October 2020.