8E COMMISSION

THE APPLICABILITY OF INTERNATIONAL LAW TO CYBER ACTIVITIES

L'APPLICABILITÉ DU DROIT INTERNATIONAL AUX CYBER ACTIVITÉS

RAPPORTEUR : VAUGHAN LOWE

La commission est composée de

Mme Mahnoush Arsanjani, M. Olivier Corten, Mmes Patrícia Galvão Teles, María Teresa Infante Caffi, MM. Bing Bing Jia, Roy S. Lee, Lauri Mälksoo, Václav Mikulka, Jin-Hyun Paik, Sergey Punzhin, Michael Reisman, Malcolm Shaw, Mme Gabriella Venturini, M. Santiago Villalpando.

I.S.B.N. 978-2-233-01042-1

PRELIMINARY REPORT

The Commission on 'the Applicability of International Law to Cyber Activities' was established by the Bureau of the *Institut de Droit international* in February 2022.

The first step in the work of the Eighth Commission was an introductory letter from the Rapporteur circulated to members of the Commission on 30 March 2022, posing some initial questions. The material part of the letter read as follows:

« Our subject is, to me at least, lacking in obvious boundaries, and I think our first task should be to try to decide upon a framework within which we will commence substantive work. There may be many ideas of what that framework should be, but please allow me to start the discussion by putting forward some initial thoughts.

I take the term 'cyber activities' to mean activities involving the use of both (i) computers and the (ii) internet. Computers operating in isolation, for example in what are now old-fashioned pocket calculators or refrigerators or cars, are thus excluded because they are not connected to the internet. (And by 'internet' I understand the entire global network connecting computers using standardized communications protocols.)

As to what those activities are, for the purposes of our work, I have no clear idea. The range of activities and legal questions is immense. Examples include cyber warfare, including both attacks on networks and the use of autonomous weapons systems; remote scientific research over the oceans; the compilation of banks of personal data; the automatization of international sales transactions; the creation of virtual reality communities in which members engage in activities that may be unlawful elsewhere; and the creation of non-State-based international currencies.

My initial thought is that, at least at this stage, we should focus on the public international law framework for the regulation of cyber activities, and focus on fundamental principles rather than on the identification of specific rules.

Five basic questions come to mind, of which the first three are probably the most fundamental:

1. Can cyber activities be regulated satisfactorily on the basis of traditional principles of jurisdiction based on territory and nationality?

With communications routed through chains of computers in different countries, possibly on routes not identified or identifiable in advance, is it practicable to allocate jurisdiction and responsibility on the basis of the (perhaps momentary) location of acts or events? Similarly, where an activity conducted via the internet may involve elements in several different States, which States have jurisdiction and responsibility? Can technology – either hardware or software – have a nationality? What happens when it is sold?

I.S.B.N. 978-2-233-01042-1

2. Can cyber activities be regulated satisfactorily by States alone or is it necessary to involve private actors?

Users of the internet are heavily dependent upon service providers, who may be alone in having direct access to the hardware and software necessary to control an activity. Service providers can change the routeing of internet communications and the locations of equipment and technology to avoid restrictive jurisdictions. Effective regulation by anyone may require the acceptance of industry-standard equipment and protocols. Is it even possible to regulate cyber activities without involving private actors in the task?

3. What should be the focus of regulation?

The internet and cyber activities could be left open and unregulated; but if there are to be regulations, what should be their focus – the thing regulated? Hardware, e.g., computers, components, cables and satellites? Software, e.g., the programs that enable the internet to carry communications, or specific programs that perform particular tasks? Activities, e.g., trafficking in illegal substances or images, maintaining 'currencies', facilitating illegal activities? Effects of activities, e.g., causing losses by fraud, violations of human rights, sedition? Persons, e.g., the corporations and other actors engaged in cyber activities, or the victims of such activities?

4. What topics are in need of regulation?

Should regulations address, at least initially, only questions covered by globally-accepted legal principles, such as certain serious crimes? What matters should be left unregulated, or left to individual States or service providers to regulate and police? Should the initial effort be to establish a framework for regulation, without focusing on the substantive rules to govern particular activities?

5. What form should regulations take?

Should the aim be for a global or regional treaty or treaties? Or for a non-binding statement of principles to which States might voluntarily subscribe? Should participation in certain aspects of cyber activities be conditional on compliance with agreed rules or principles? Would an international organization to oversee cyber activities be a help or a hindrance?

Can we exchange views on any or all of these five points, plus the question

Is there any other aspect that should be included in our initial study? »

RESPONSES TO THE CIRCULAR OF 30 MARCH 2022

The initial responses from members of the Commission to these questions were broad and varied. At this preliminary stage there is little advantage in reproducing these initial responses in their entirety. All members of the Commission were copied in on each of the responses, which have been compiled into a single document, 'Initial responses to first introductory email', in the Eighth Commission's folder on the *Institut*'s website. The following paragraphs summarize the responses.

I.S.B.N. 978-2-233-01042-1

The main topics identified in the responses as needing to be addressed included the following: the definition of the concept of a 'cyber activity', and the clarification of the terminology used in its legal analysis; the current engagement with cyber activities by existing international organizations; State practice in matters relating to cyber activities; the adequacy of the traditional framework of public international law in relation to cyber activities; the extent of State responsibility for cyber activities; the role of the private sector in regulating cyber activities; and the identification of specific topics, such as the law of war, human rights law, the concepts of sovereignty and non-intervention, and foreign investment, that give rise to particular issues concerning cyber activities.

In general, there were few signs of any fundamental differences at this stage among the Commission members concerning the approach to be adopted. On the contrary, there appears to be a convergence of views on the central issues.

The responses indicate a general acceptance (a) that the definition of 'cyber activities' offered in the 30 March 2022 circular – 'activities involving the use of both (i) computers and (ii) the internet (i.e., the entire global network connecting computers using standardized communications protocols)' – can be used as a working definition; (b) that international law is applicable to 'cyber space', understood as a metaphor for cyber activities in general; and (c) that the Commission should, at least initially, proceed with its work within the framework of public international law.

There appears to general agreement that the Commission should not aim to draw up rules for the governance of the internet, nor substantive rules applicable to specific cyber activities covered by particular areas of international law. Rather, the Commission should focus on the clarification of concepts and the identification an articulation of general legal principles underlying specific rules, notably the principles concerning State responsibility and jurisdiction. In that context, it is helpful to focus initially upon wrongful conduct in breach of international law or municipal law, as this conduct engages the simplest and paradigmatic exercises of State authority. Other juridical acts, such as those altering the status of a legal person or creating legal persons or rights or property, may be addressed later.

It is also accepted that the "international law applicable to cyber activities" must fit in with the body of general international law applicable to non-cyber activities. Indeed, that statement puts the matter the wrong way round: international law *is* applicable to 'activities' and there is no exception for activities performed using cyber techniques and equipment. 'Cyberspace' is at least primarily a metaphor, not a distinct conceptual space with its own juridical order.[1]

An important associated point emphasised in several responses is that there should be no presumption that the existing rules of international law are inadequate to deal with cyber activities or that new rules are needed. Any such need must be

[1] Though the term might also be applied to the imagined worlds of video games and virtual reality, where those who control the games and scenarios may devise and enforce specific rules against those participating in such games and scenarios.

I.S.B.N. 978-2-233-01042-1

carefully identified and established; and it may be that in some, or even all areas examined by the Commission the wisest conclusion is that given the present stage and rate of developments in technology and in State practice, the time for identifying applicable legal principles is not yet ripe.

The responses mostly addressed matters in general terms, not directed to specific questions in the 30 March 2022 circular. Nonetheless, a brief summary of the implications of the responses for each of the questions may be helpful.

Can cyber activities be regulated satisfactorily on the basis of traditional principles of jurisdiction based on territory and nationality?

It is apparent that underlying many, if not all, of the questions that arise in relation to cyber activities is the problem of determining when and where a cyber event occurs and to whom it is to be attributed. The answers to those questions are foundations on which rules of jurisdiction and international responsibility rest. These matters are addressed further in the next section.

Can cyber activities be regulated satisfactorily by States alone or is it necessary to involve private actors?

There is a consensus that the Commission should not attempt to create a novel framework for the regulation of cyber activities, analogous to 'environmental law' or 'the law of the sea'. The allocation among organizations, including State bodies, of responsibilities for the governance of cyberspace can probably be set aside, at least at this stage of the Commission's work. It is therefore proposed to omit the question of the involvement of private actors in the actual regulation of cyber activities from the list of questions that the Commission will address directly as distinct topics.

That said, the involvement of private actors and other non-State entities will be immediately relevant to other questions addressed by the Commission. For instance, where cyber activities occur within networks or other facilities provided or hosted by commercial companies, the definition of the circumstances in which State responsibility arises in the context of the conduct or inaction of such companies is a matter fundamental importance.

What should be the focus of regulation?

When this question was asked on 30 March 2022, the possibility was kept open of the Commission working on a framework for regulating cyber activities. The general view in the responses to the initial questions is, however, that the Commission should not focus on the question of substantive regulations directly applicable to cyber activities – a kind of "international law of cyber activities" – and so that aspect of the matter is best put aside. The specific points raised in the longer text of this question (set out above), however, remain, and they are fundamental to any consideration of how international law addresses cyber activities.

I.S.B.N. 978-2-233-01042-1

What topics are in need of regulation?

As has been noted, there is an apparently general view that the Commission should not focus on the question of substantive regulations directly applicable to cyber activities. This question loses its pertinence if the Commission proceeds on the basis of that view.

What form should regulations take?

The question of the form that international regulations should take also loses its pertinence if the Commission does not address substantive regulations applicable to cyber activities.

Is there any other aspect that should be included in our initial study?

It appears to be generally accepted that the initial aim of the Commission should be to clarify legal concepts, terminology, and issues, and to identify broad principles, and not to set out any detailed blueprint for the regulation of cyber activities. On that basis the specific inclusion of particular legal aspects of cyber activities, such as cyber crime or cyber combat, within the study at this stage seems unnecessary and inappropriate.

On the other hand, the location and consideration of State practice in relation to cyber activities, which is an aspect of the subject identified in several responses, can usefully be pursued alongside the Commission's initial work. A basis for this exercise already exists in the UN Official compendium of voluntary national contributions on the subject of how international law applies to ICT.[2]

THE NEXT STEPS FOR THE EIGHTH COMMISSION

The *Institut* has not discovered cyberspace. It is not even among the first wave of cartographers to land on its shores, intent on mapping the relationship between cyberspace and international law. Cyber activities have now been a subject of serious attention within international law for some decades. Among the landmarks in the early history of the topic (to use a metaphor mixing space and time, which could itself stand as a metaphor for some of the basic problems with which cyber activities confront international law) are the 2000 EU Directive on Electronic Commerce,[3] the 2001 Budapest Convention on Cybercrime,[4] the establishment of

[2] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266,* UN Doc. A/76/136*; < https://undocs.org/en/A/76/136 >.

[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), < https://eur-lex.europa.eu/legal-content/EN/ALL/?uri =CELEX %3A32000L0031 >

[4] Council of Europe, Convention on Cybercrime (ETS No. 185). Budapest, 23 November 2001; see < https://www.coe.int/en/web/cybercrime/home >.

I.S.B.N. 978-2-233-01042-1

the UN Internet Governance Forum ('IGF') in 2006,[5] and in 2013 the first edition of the Tallinn Manual the International Law Applicable to Cyber Warfare.[6] Work continues apace. In 2021 the UN Group of Governmental Experts ('GGE'), first established in 2004, submitted its final report on advancing responsible State behaviour in cyberspace in the context of international security,[7] while the UN Open-Ended Working Group on security of and in the use of information and communications technologies ('OEWG'), established in 2018, began its second mandate (2021-2025).[8] In the same year the NATO Cooperative Cyber Defence Centre of Excellence ('CCDCOE') began its five-year project to produce the third edition of the Tallinn Manual.[9] There are also private initiatives. For instance, in 2017 Microsoft launched a call for a Digital Geneva Convention, with a particular focus on the duty to protect civilian uses of the internet.[10]

A great deal of work on the relationship between cyber activities and Law has been done over the past quarter-century by such organizations and by individuals. Furthermore, there is important ongoing work that includes among its specific focuses the question of the applicability of international law to cyber activities. While that may still be in the early stages of its development, it is the subject of an established and continuing conversation which has already given rise to some accepted principles and common understandings. An immediate question is how best the *Institut* might engage with that conversation.

As a practical matter, the 2021 report by the GGE[11] offers a convenient route in to the area of the work of the Eighth Commission. Within the UN the focus has been on 'information and communication technologies (ICTs)'. The concept of ITCs is not exactly coextensive with cyber activities. because it also includes radio and television broadcasting and telephony, for example.[12] Nonetheless, ICT is the wider concept, embracing all cyber activities; and the work of the GGE, like that of the OEWG, is directly relevant to the work of the Eighth Commission. Among the specific topics that the GGE has addressed are "norms, rules and principles for the responsible behaviour of States" and "how international law applies to the use of ICTs".[13]

The 2021 report provides a useful overview of the GGE's work. In 2015, the GGE adopted eleven voluntary, non-binding norms of responsible State behaviour,[14] including norms that bear upon questions of international law. In

[5] See < https://www.intgovforum.org/en >
[6] See now < https://ccdcoe.org/research/tallinn-manual/ >.
[7] See < https://www.un.org/disarmament/group-of-governmental-experts/ >. The GGE made Reports in 2010 [UN Doc. A/65/201], 2013 [A/68/98*], 2015 [A/70/174], and 2021 [A/76/135].
[8] See < https://www.un.org/disarmament/open-ended-working-group/ >
[9] < https://ccdcoe.org/research/tallinn-manual/ >
[10] See < https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/ >; < https://news.microsoft.com/cloudforgood/policy/briefing-papers/trusted-cloud/creating-digital-geneva-convention.html >.
[11] UN Doc. A/76/135, 14 July 2021.
[12] See the UNESCO definition of ICT: < https://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict >.
[13] See the 2021 GGE Report, UN Doc. A/76/135, pp. 8–18.
[14] UN Doc. A/70/174, 22 July 2015. See pp. 7–8.

I.S.B.N. 978-2-233-01042-1

resolution 70/237 the General Assembly called upon States to be guided in their use of ICT by the 2015 report,[15] in which the norms were set out. The norms were subsequently developed by the GGE and are set out in their current iteration in the GGE 2021 report. Implementation of the norms is being monitored.[16] They are pitched at a high level of generality: for example, "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[17] Similarly, on the question of how international law applies to cyber activities the GGE affirmed that "adherence by States to international law, in particular their [sc., UN] Charter obligations, is an essential framework for their actions in their use of ICTs."[18]

This generality offers an opportunity for a significant contribution by the *Institut*. The application of general norms and principles such as those articulated by the GGE to specific circumstances gives rise to critical and fundamental questions. Consider the hypothetical example of a lone individual, unaffiliated to any government, in State A who launches a computer virus as an attachment to an email sent simultaneously to thousands of email addresses in scores of States around the world that have been procured by hacking a commercial site on the internet that is hosted on a server physically located in State B. The email is transmitted, on a route determined automatically by pieces of equipment, supplied by companies in State C, located in a large number of States around the world. The equipment is operating automatically on the basis of computer programs supplied by companies in State D which include affiliates of the companies that supplied the equipment. The virus, once activated by a recipient of an email, re-transmits itself from the recipient's computer to other email addresses stored in that computer, and attaches itself to that computer's calendar program with an instruction to delete all the computer's data one month after the virus is implanted in the computer. As a result, computers in almost all States in the world, belonging to individuals, institutions such as hospitals, and emergency services, become infected and fail. In such circumstances, which State(s) can exercise jurisdiction, and which State(s) incur responsibility under international law and for what acts and/or omissions?

Such scenarios give rise to both legal and technical questions. For instance, as a matter of law, which States (if any) are 'knowingly allowing use of their territory' in situations where, after its existence and characteristics are known, the virus continues to proliferate via servers located in the respective territories of the States? One's instinctive answer to that question may be influenced by the image that one has of the transmission from server to server of the data package containing the virus, by internet cable or by satellite signal or by other means, such as telephony or the physical transfer of storage devices such as USB sticks. If transmission is envisaged as being like a tree branch thrown into an international

[15] See UN GA resolution 70/237, and the 2021 GGE Report, UN Doc. A/76/135, pp. 8–17.
[16] See < https://nationalcybersurvey.cyberpolicyportal.org/wp-content/uploads/2022/01/empty_survey.pdf >
[17] 2021 GGE Report, UN Doc. A/76/135, p. 10, Norm 13(c).
[18] 2021 GGE Report, UN Doc. A/76/135, p. 17, paragraph 69.

I.S.B.N. 978-2-233-01042-1

river and drifting downstream, the identity, sequence and limits of the 'territorial' States are fairly easily identified (though difficulties may arise if an international border follows the course of the river, and the branch drifts unpredictably from one side to the other). If transmission is envisaged like the passage of a message between semaphore stations or the lighting of fire beacons, the position is less obvious. Or perhaps the transmission of the data by electrons[19] along a cable is imagined as being like a pipe full of contiguous ball bearings stretching across international borders, with the pushing of one more ball bearing into the pipe, resulting in the movement of a ball bearing at the other end of the pipe (and every one of the intervening bearings) by the breadth of one ball bearing, but with no 'thing' actually moving along the row at all. Does it make any difference which of those imagined pictures of internet traffic is closest to what is understood to be the scientific 'truth'? What, if anything, 'occurs' in the States along the route to the addressee(s) of the data, and what rights and responsibilities does each of those States have? Should the movement of data between servers in different States be thought of as being akin to the exercise of freedom of navigation or of the right of innocent passage or of transit passage through the seas, or as being closer to an international car journey, crossing permitted borders on production of necessary visas? To what extent is the right of each State to regulate the transmission (for instance, by shutting down an internet cable or network, or ordering its commercial owner to do so) constrained its obligations owed to third States?

As a technical matter, is it actually possible to identify and intercept a data package containing a virus while it is 'travelling' across the internet? Or is that possible only when the package has come to rest, as it were, in a computer? Is it possible to block internet traffic coming from State A into State B, but without stopping incoming traffic from other States? Is that something that a State can superimpose on the internet, or is it something that only the owners and operators of the network of cables and radio signals can do, either on their own initiative or under the orders of one State or another?

The more one digs in to these questions, the more the evident it becomes that the application of traditional rules and principles of international law to cyber activities is far from being a straightforward matter. Much work has already been done on the complexities of the position in the context of the law of armed conflict; but the problems are general, pervasive, and ultimately unavoidable. Much remains to be done.

The Eighth Commission might embark upon a two-stage study. The first stage would address the question, when and where does an act or omission occur in the context of cyber activities, and in what circumstances does a State incur international responsibility for such an act or omission? That rather dense formulation of the question is broadly intended to embrace the matrix of questions

[19] One estimate suggested that the data flowing over the internet is carried by no more than around 60 grams of electrons, or perhaps as little as 6 micrograms of electrons:
< https://www.theguardian.com/technology/2007/jun/07/guardianweeklytechnologysection1 >.

I.S.B.N. 978-2-233-01042-1

addressed in the ILC's Articles on the Responsibility of States for Internationally Wrongful Acts, and particularly those in Part One ("The Internationally Wrongful Act of a State') and Articles 46 ("Plurality of injured States") and 47 ("Plurality of responsible States").

One way of approaching the question is to begin by considering a range of paradigmatic hypothetical situations and trying to discern the principles running through the preferred legal analyses. The UNIDIR publications on the 'Taxonomy of Malicious ICT Incidents',[20] and the scenarios annexed to the Australian response to the UN request for submissions on the subject of how international law applies to ICT,[21] may be found helpful in this context.

The second stage of the Commission's work would consider whether, given the response to the first question, the traditional framework of international law is adequate for application to cyber activities.

In addition, the second stage might take on the question whether the exercise of jurisdiction, and perhaps the imposition of responsibility, on the basis of the nationality of technology is possible and appropriate. That question has already attracted much attention in the context of the imposition of export controls by States, and notably by the USA;[22] and because nationality (unlike space and time, as the underlying components of territorial jurisdiction) is in this context a purely legal construct and accordingly malleable, and also because the need for reliance on nationality and other bases of jurisdiction will become clearer once the potential and limitations of territorial jurisdiction have been explored, this topic is probably best excluded from the stage one inquiry.

At each stage, the Commission can consider not only the question whether jurisdiction and responsibility exist in certain circumstances, but also how the answer is best framed and the legal position best described.

There are many legal concepts that might be used or adapted to express the position. For example, jurisdiction is not a binary concept, either existing or not. A coastal State has jurisdiction over foreign ships when they are in the State's ports and other internal waters, and when they are stationed in or engaged in innocent passage through the territorial sea, and when they are engaged in transit passage, and when they are in the State's Exclusive Economic Zone. But the 'jurisdiction' is by no means the same in every case. It varies not only from one

[20] Samuele Dominioni, Giacomo Persi Paoli, A Taxonomy of Malicious ICT Incidents (UNIDIR, 2022), < https://www.unidir.org/publication/taxonomy-malicious-ict-incidents >, and 'Annex: List of taxonomies and other classifications of cyber acts' (UNIDIR, 2022) < https://unidir.org/sites/default/files/2022-11/UNIDIR_Taxonomy_Malicious_ICT_Incidents_Annex.pdf >.

[21] *Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266,* UN Doc. A/76/136*, p. 3 at pp. 8-12; < https://undocs.org/en/A/76/136 >.

[22] For a recent study see chapters 5 and 11 by Joop Voetelink in the Netherlands Annual Review of Military Studies 2021, *Compliance and Integrity in International Military Trade*: < https://link.springer.com/content/pdf/10.1007/978-94-6265-471-6.pdf?pdf=button%20sticky >.

I.S.B.N. 978-2-233-01042-1

maritime zone of the State to another, but also according to whether the ship is or is not engaged in passage, and whether it is or is not conforming to any conditions imposed on that passage, and to the purposes for which and the circumstances in which the State is exercising jurisdiction. Thus, States may enact for ships in innocent passage laws regarding the control of pollution; but in the case of laws applying to the design construction, manning or equipment of foreign ships they may do so only if the laws give effect to generally accepted international rules or standards. The enforcement of laws is, moreover, constrained by further rules of international law and by principles of international comity.[23]

Even the language of rights and duties has its alternatives, or at least its variations. To take another possible model, Article XXIII:1 of GATT 1994 provides for the invocation of the dispute settlement system not simply in circumstances where one State alleges that its legal *rights* have been violated, but also where it considers that "any benefit accruing to it directly or indirectly" under the Agreement is being nullified or impaired as a result of another contracting party failing to carry out its obligations.

While a State either does or does not carry international responsibility in any specific case, even the notion of responsibility is not two-dimensional: it has its gradations and contours. The principles reflected in the ILC articles on participation in, or aiding or assisting, the conduct of other States, and the ILC provisions on pluralities of injured and responsible States, all offer possibilities for a legal analysis of cyber activities that is more appropriate for the complexities and subtleties of the international relationships that such activities involve than a simple statement that State A is or is not responsible for a given cyber act.

The identification for the purposes of international law of a precise definition of cyber activities and of when and where they occur and of the circumstances in which they entail international responsibility is a task of considerable difficulty, which may require a reconsideration of the basic notions of 'acts' and 'agency' which international law has accepted for centuries. This is the almost inevitable result of the introduction into routine international transactions of automated processes, owned and most immediately controlled by private actors, which processes may operate in a manner that is for practical purposes both unpredictable and not susceptible to real-time monitoring and supervision. Incoming internet traffic cannot be monitored and tracked in the way that, say, an incoming missile can be.

It is accordingly proposed that the Eighth Commission should begin its work by considering these basic questions. Specifically, it is proposed that at the Angers session of the *Institut* the Commission should meet to consider the questions, **when and where does an act or omission occur in the context of cyber activities, and in what circumstances does a State incur international responsibility for such an act or omission?** Members of the Commission are invited to circulate their views on this proposal and their comments on this

[23] UN Convention on the Law of the Sea, Article 21. See further R. Churchill, V. Lowe and A. Sander, *The Law of the Sea* (4th ed., 2022) chs. 3, 5, 6, 7, 9.

I.S.B.N. 978-2-233-01042-1

preliminary report and on the topic more generally. A short virtual meeting will be arranged in the Spring of 2023 to settle the agenda for the Angers meeting and any other preliminary matters.

This preliminary report is available in the Eighth Commission folder on the intranet link of the *Institut*'s internet site, which can be accessed by going to < https://www.idi-iil.org/en >, and clicking on the extranet link < https://intra.justitiaetpace.org/login.php?phpgw_forward=%252Findex.php >, along with some of the materials to which it refers.

I.S.B.N. 978-2-233-01042-1