International Review of the Red Cross (2022), **104** (919), 1171–1198.
Selected Articles
doi:10.1017/S1816383122000091

IRRC

Hacking international organizations: The role of privileges, immunities, good faith and the principle of State sovereignty

Russell Buchan and Nicholas Tsagourias*
Russell Buchan is Senior Lecturer in International Law at the University of Sheffield.

Nicholas Tsagourias is Professor of International Law at the University of Sheffield.

Abstract
This article examines the extent to which international law protects international organizations (IOs) from hacking operations committed by States. First, it analyzes whether hacking operations undertaken by member States and host States breach the privileges and immunities granted to IOs by their constitutive treaties, headquarters agreements, and conventions on privileges and immunities concerning the inviolability of their premises, property, assets, archives, documents and correspondence. The article also explores the question of whether hacking operations carried out by non-member States breach these provisions on the basis that they have passed into customary international law or because they attach to the international legal personality of IOs. Second, the article considers the question of whether hacking operations breach the principle of good faith. In this regard, it discusses the applicability of the principle of good faith to the relations between IOs, member States, host States and non-member States, and then considers how

* The authors would like to thank Daniel Franchini for his comments on a previous draft of this article. Any errors remain the responsibility of the authors.

hacking operations impinge on a number of postulates emanating from good faith such as the pacta sunt servanda rule, the duty to respect the legal personality of IOs, the duties of loyalty, due regard and cooperation, and the duty not to abuse rights. Finally, the article examines the question of whether the principle of State sovereignty offers IOs indirect protection insofar as hacking can breach the sovereignty of the host State or the sovereignty of the State on whose cyber infrastructure the targeted data is resident.

Keywords: international organizations, hacks, data protection, privileges and immunities, good faith, State sovereignty.

Introduction

International organizations (IOs) increasingly collect, store, process, analyze, exchange and communicate information as part of their daily activities. One type of information handled by IOs is the personal information of employees, and IOs usually have specific rules, policies and procedures in place to regulate how this information is used.[1] Another type of information handled by IOs, and which is our focus in this article, relates to the exercise of their powers and the discharge of their functions. For example, IOs use information to monitor sanctions and ceasefires, enforce arms control regimes, protect civilians against attacks, identify international humanitarian law and international human rights law violations in the course of peacekeeping operations, make decisions, plan and execute operations, counter terrorism and prevent diseases. This information is gathered, analyzed, stored, shared and communicated in the course of an IO's decision-making cycle and activities. Ensuring the confidentiality, availability and integrity of this information is important for the functioning of IOs and their ability to carry out their tasks effectively.[2]

In the modern era, the information collected and handled by IOs is almost invariably compiled as electronic data. Inevitably, IOs have become the target of hacking operations – that is, cyber operations which gain access to data that is resident on computer networks and systems without the consent of the IO and which do not serve any lawful purpose under international law. For example, officials of United Nations (UN) bodies mandated to monitor the sanctions imposed on North Korea have been targeted by spear-phishing attacks attributed

1 See UN High-Level Committee on Management, *Principles on Handling of Personal Information*, October 2018, available at: https://unsceb.org/personal-data-protection-and-privacy-principles (all internet references were accessed in February 2022).

2 See, for example, Office of the UN High Commissioner for Refugees, *Policy on the Protection of Personal Data of Persons of Concern to UNHCR*, May 2015, available at: www.refworld.org/docid/55643c1d4.html; UN, *Data Strategy of the Secretary-General for Action by Everyone, Everywhere 2020–2022*, 2020, available at: www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf.

to North Korea's Kimsuky advanced persistent threat group.[3] Reports also demonstrate that dozens of UN servers – including those operated by the UN's human rights offices – have been hacked.[4] The UN is not the only IO that has fallen victim to attempted hacking; many other IOs, regardless of their designation, have been targeted. In 2018, the Netherlands foiled a hack against the Organisation for the Prohibition of Chemical Weapons (OPCW) and attributed it to Russia.[5] At the time, the OPCW was investigating the poisoning of former Russian double agent Sergei Skripal and his daughter Yulia Skripal as well as a chemical attack on the Syrian city of Douma. During the COVID-19 pandemic, the World Health Organization (WHO) reported that there had been a sharp rise in attempts to hack its computer networks and systems and gain access to sensitive data.[6] In January 2022, the International Committee of the Red Cross (ICRC)[7] reported that its data had been hacked while the data was stored on servers hosted by a private company based in Switzerland.[8] The ICRC determined that the personal information of more than 500,000 people receiving services from the International Red Cross and Red Crescent Movement had been compromised and that it was working under the presumption that this data had been "copied and exported".[9]

Although hacking has become a widespread feature of international affairs, academic attention has largely focused on whether and to what extent international law protects *States* from hacking.[10] Little – if any – academic literature has analyzed whether international law protects *IOs* from hacking, even though they exercise

3 *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, UN Doc. S/2020/840, 28 August 2020, paras 118–121. See also *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, UN Doc. S/2020/151, 2 March 2020, Annexes 28–30.

4 "The Cyber Attack the UN Tried to Keep under Wraps", *The New Humanitarian*, 29 January 2020, available at: www.thenewhumanitarian.org/investigation/2020/01/29/united-nations-cyber-attack; "United Nations Agency 'Hacking Attack' Investigated", *BBC News*, 21 November 2021, available at: www.bbc.co.uk/news/technology-15951883.

5 "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation Targeting OPCW", *ASD News*, 4 October 2018, available at: www.asdnews.com/news/defense/2018/10/04/netherlands-defence-intelligence-security-service-disrupts-russian-cyber-operation-targeting-opcw.

6 WHO, "WHO Reports Fivefold Increase in Cyber Attacks, Urges Vigilance", 23 April 2020, availabe at: www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance; "Elite Hackers Target WHO as Coronavirus Cyberattacks Spike", *Reuters*, 23 March 2020, available at: www.reuters.com/article/us-health-coronavirus-who-hack-exclusive-idUSKBN21A3BN.

7 In the authors' view, the ICRC is an international organization possessing international legal personality. Various States and IOs have recognized the ICRC's international legal personality; for a discussion of this practice, see Els Debuf, "Tools to Do the Job: The ICRC's Legal Status, Privileges and Immunities", *International Review of the Red Cross*, Vol. 97, No. 897–898, 2015, pp. 321–329.

8 ICRC, "Cyber-Attack on the ICRC: What We Know", 21 January 2022, available at: https://icrc.org/en/document/cyber-attack-icrc-what-we-know; ICRC, "ICRC Cyber-Attack: Sharing our Analysis", 16 February 2022, available at: www.icrc.org/en/document/icrc-cyber-attack-analysis.

9 *Ibid.* ("Were data sets copied and exported? We must presume so. We know that the hackers were inside our systems and therefore had the capacity to copy and export it.")

10 See, generally, Russell Buchan, *Cyber Espionage and International Law*, Hart, Oxford, 2018; Russell Buchan and Iñaki Navarrete, "Cyber Espionage and International Law", in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace*, Edward Elgar, Cheltenham, 2021; Asaf Lubin, "The Liberty to Spy", *Harvard International Law Journal*, Vol. 61, No. 1, 2020; Craig Forcese, "Spies Without Borders: International Law and Intelligence Collection", *Journal of National Security Law and Policy*, Vol. 5, No. 1, 2011.

important governance functions and handle large amounts of data. With this in mind, this article is perhaps the first to examine the important and timely question of which international legal rules apply when IOs fall victim to hacking operations committed by States. In answering this question, we identify three types of hacking scenarios: the first involves hacking by member States (MSs) of the IO in question, the second involves hacking by States that host the IO within their territory (host States), and the third involves hacking by non-member States (NMSs) of the IO in question.[11]

All three scenarios give rise to a number of overlapping legal issues. The first of these concerns the scope of the privileges and immunities accorded to IOs by their founding treaties, headquarters agreements, conventions on privileges and immunities, and customary international law (CIL), and whether hacking by MSs, host States and NMSs breaches these obligations. The second issue concerns the application of the principle of good faith (GF) to the relations between IOs, MSs and NMSs, and whether hacking breaches the particular legal postulates that stem from this principle and govern these relations. The third issue concerns the scope of the principle of State sovereignty and whether hacking breaches the sovereignty of the host State or the State on whose infrastructure the IO's data resides.

The ensuing legal analysis follows the above order, and its principal aim is to explain how the aforementioned regulatory frameworks protect IOs from hacking. This study is important because it identifies the basic set of legal parameters that should be considered when IOs are hacked, and the analysis herein will help scholars and practitioners better understand and evaluate the effectiveness of legal responses to this issue.

International organizations and their privileges and immunities

States establish IOs in order to pool resources and achieve certain objectives through joint and coordinated action. Because IOs exercise governance functions over States but consist of States which retain their sovereignty, they require a range of privileges and immunities to enable them to operate free from interference. Privileges and immunities refer to certain protections and exemptions from local jurisdiction that are necessary for the independent functioning of IOs and the effective performance of their tasks.[12] This section therefore examines the source and

11 In this article, we assume that the hacking is committed by a State or is attributable to a State. On attribution in the context of IOs, see International Law Commission (ILC), *Draft Articles on the Responsibility of International Organizations*, 2011 (DARIO). On cyber attribution, see Nicholas Tsagourias and Michael Farrell, "Cyber Attribution: Technical and Legal Approaches and Challenges", *European Journal of International Law*, Vol. 31, No. 3, 2020.

12 "Both the basis for and the scope of this immunity, which is aimed at ensuring that the UN can function completely independently and thus serves a legitimate purpose, are therefore different from those underlying the immunity from jurisdiction of foreign states": Supreme Court of the Netherlands, *Stichting Mothers of Srebrenica and Others v. Netherlands and United Nations*, LJN: BW1999, ILDC 1760 (NL, 2012), Final Appeal Judgment, 13 April 2012, para. 4.2. "International organizations enjoy

scope of these privileges and immunities and assesses whether and to what extent they protect IOs from hacking.

Privileges and immunities under conventional law

The constitutive treaties of IOs usually grant IOs certain privileges and immunities vis-à-vis their MSs, but IOs may also conclude additional agreements that set out in more detail the nature, content and scope of those privileges and immunities. For example, Article 105(1) of the UN Charter states that the UN "shall enjoy in the territory of each of its Members such privileges and immunities as are necessary for the fulfilment of its purposes", whereas the 1946 Convention on the Privileges and Immunities of the United Nations (CPIUN) fleshes out the detail of the UN's privileges and immunities.[13]

As already indicated, the basis of the privileges and immunities of IOs is functional necessity, and given that IOs possess different functions, they would in principle require different privileges and immunities. That said, IOs are usually endowed with broad and general functions which are interpreted and reinterpreted as the international political landscape evolves.[14] The upshot of this is that, in practice, the concept of functional necessity often leads to the award of general or "absolute" privileges and immunities.[15]

When formulating their agreements on privileges and immunities, IOs tend to use the CPIUN as a model.[16] In this way, the CPIUN has "become *the* reference point for the definition of the privileges and immunities of other IOs".[17] Also, many of the concepts appearing in the CPIUN – such as the terms "premises", "inviolable", "archives" and "documents" – are used by the 1961 Vienna

privileges and immunities entirely because they are necessary for the fulfilment of their purposes and functions": Chittharanjan Felix Amerasinghe, *Principles of the Institutional Law of International Organizations*, Cambridge University Press, Cambridge, 2006, p. 316. See also C. Wilfred Jenks, *International Immunities*, Stevens & Sons and Oceana, London, 1961, p. 18; Council of Europe, Committee of Ministers, *European Committee on Legal Cooperation: Addendum: Privileges and Immunities of International Organizations and Persons Connected with Them*, 9 July 1969, p. 4; Chanaka Wickremasinghe, "International Organizations or Institutions: Immunities before National Courts", *Max Planck Encyclopedia of International Law*, 2009, para. 1.

13 In relation to the UN's specialized agencies, see Convention on the Privileges and Immunities of Specialized Agencies, 1947.

14 August Reinisch, "Privileges and Immunities", in Jacob Katz Cogan, Ian Hurd and Ian Johnstone (eds), *The Oxford Handbook of International Organizations*, Oxford University Press, Oxford, 2016, p. 1058.

15 "[T]he immunity of international organizations, within the framework of their functional restrictions, is to be regarded in principle as absolute": Austrian Supreme Court, *Firma Baumeister Ing. Richard L v. O*, 10 Ob 53/04 y, ILDC 362 (AT 2004), 14 December 2004, para. 12. See also August Reinisch and Peter Bachmayer, *The Convention on the Privileges and Immunities of the United Nations and Its Specialized Agencies: A Commentary*, Oxford University Press, Oxford, 2016, p. 67 ("In practice an unqualified, general immunity … is often regarded as absolute immunity").

16 See, for example, General Agreement on Privileges and Immunities of the Council of Europe, 1949; Agreement on Privileges and Immunities of the Organization of American States, 1949; Treaty Establishing the Central American Institute of Public Administration, 1954; Agreement Establishing the World Trade Organization, 1995; Convention on the Privileges and Immunities of Specialized Agencies, 1947.

17 E. Debuf, above note 7, p. 333.

Convention on Diplomatic Relations (VCDR) to describe the privileges and immunities of diplomatic missions. Courts[18] and commentators[19] have thus used these definitions to interpret the privileges and immunities of IOs under the CPIUN. Consequently, we will examine specific provisions of this agreement in order to consider how they apply to incidents of hacking.

Section 3 of the CPIUN provides that "[t]he premises of the United Nations shall be inviolable". The term "premises" refers to those areas that house or contain an IO and includes those spaces owned, occupied or controlled by the organization,[20] such as buildings (and parts thereof), car parks and gardens. The premises of an IO can be virtual insofar as they include the computer networks and systems that are supported by cyber infrastructure which is physically located within the organization's premises.[21] Generally, the premises of IOs do not extend to computer networks and systems hosted by cyber infrastructure located beyond the IO's physical premises – for example, where computer systems and networks are supported by servers located within the territory of the host State or third States.[22] However, where an IO can establish ownership or control over that computer network or system, it will form part of the organization's "premises". An IO's ownership of a computer network or system may be indicated by the fact that it has entered into a contract with a service provider that grants legal ownership to the organization. An IO exercises control over a computer network or system where, for example, it regulates access to that network or system (e.g., by deploying and operating firewalls and anti-intrusion software) and supervises the activities occurring within it. Regarding the 2022 ICRC hack, the ICRC explained that it manages the data and applications on the targeted servers notwithstanding the fact that they are hosted by a private company.[23] The ICRC therefore exercises control over the servers and, on this basis, they can be said to form part of the ICRC's premises and as such are protected from hacking.

Premises are "inviolable" to the extent that they are protected from any form of interference.[24] International law therefore deploys a "protective ring"

18 Supreme Court of Canada, *World Bank Group v. Wallace*, [2016] 1 SCR 207, 29 April 2016, para. 78.

19 Laurie Blank, "The Limits of Inviolability: The Parameters for Protection of United Nations Facilities during Armed Conflict", *International Law Studies*, Vol. 93, 2017, p. 55.

20 UN General Assembly, *The Practice of the United Nations, the Specialized Agencies and the International Atomic Energy Agency concerning their Status, Privileges and Immunities: Study Prepared by the Secretariat*, UN Doc. A/CN.4/L.118, 8 March 1967. See also A. Reinisch and P. Bachmayer, above note 15, p. 127.

21 With regard to the diplomatic and consular missions of States, some authors have argued that their premises encompass the computer networks and systems supported by cyber infrastructure that is located within the missions' physical premises. See Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual 2.0), Rule 39; R. Buchan, above note 10, p. 73.

22 R. Buchan, above note 10, p. 73.

23 "We also feel it is important to clarify that this was a targeted, direct cyber-attack on ICRC servers, not the company that hosted them. We manage the data and applications on these servers, not the hosting company": ICRC, "Cyber-Attack on the ICRC", above note 8.

24 Supreme Court of Canada, *World Bank Group*, above note 18, para. 78.

around an IO's premises and shelters them from intrusion.[25] This *cordon sanitaire* prohibits spying within the premises of IOs, and indeed, on several occasions the UN Secretariat has claimed that electronic surveillance against its offices represents a breach of its inviolability.[26] It follows that hacking operations against an IO's computer networks and systems constitute a prohibited interference in its premises and, accordingly, amount to a breach of its privileges and immunities.

Section 3 of the CPIUN also provides that "[t]he property and assets of the United Nations, wherever located and by whomsoever held, shall be immune from search, requisition, confiscation, expropriation and any other form of interference, whether by executive, administrative, judicial or legislative action". "Property and assets" include those items over which IOs can establish ownership or control.[27] They certainly include an IO's *tangible* property and assets, and this means that computer hardware such as servers and storage devices are protected from interference. But "property and assets" also include an IO's *intangible* property and assets, such as its bank accounts[28] and pension funds.[29] If this is the case, computer networks and systems and data can be "property and assets" of an IO, provided of course that the organization can establish ownership or control over them. Again, ownership of a network, system or data may be determined by the contractual relationships entered into by the IO, and control can be established where the organization exercises a regulatory and supervisory function over them. As "property and assets" of the IO, computer networks and systems and data are protected from hacking given that this activity constitutes a prohibited "search" or "interference".

Moreover, an IO's "property and assets" are protected "wherever located and by whomsoever held". This means that, where an IO is able to establish ownership or control over computer networks and systems supported by cyber infrastructure located within the territory of the host State or any other State, and regardless of whether that infrastructure is publicly or privately owned or operated, the networks and systems qualify as "property and assets" of the IO and are protected from interference. In relation to the 2022 ICRC hack, for example, the ICRC was responsible for managing the data and applications on the targeted servers rather than the private company that hosts them. The ICRC therefore exercises control over the computer networks and systems and data

25 UK Court of Appeal, *R (Bancoult No. 3) v. Secretary of State for Foreign and Commonwealth Affairs*, [2014] EWCA Civ. 708, 23 May 2014, para. 58.

26 "UN to Investigate GCHQ, MI5 Spying on Foreign Delegates at Climate Summit Talks", *RT*, 5 November 2010, available at: www.rt.com/uk/202147-uk-climate-summit-spying/; "U.N. to Britain: If Spying on Us, Stop It", *UPI*, 26 February 2004, available at: www.upi.com/Defense-News/2004/02/26/UN-to-Britain-If-spying-on-us-stop-it/31241077833950/; UN, *Daily Press Briefing by the Office of the Spokesman for the Secretary-General*, 29 November 2010, available at: www.un.org/press/en/2010/db101129.doc.htm.

27 A. Reinisch and P. Bachmayer, above note 15, p. 132.

28 *Report of the Commissioner-General of UNRWA to the General Assembly, 1 January to 31 December 2013*, UN Doc. A/69/13, 2014, para. 58.

29 Supreme Court of the State of New York, Appellate Division, *Shamsee v. Shamsee*, 428 NYS2d 33, 36 (2d Dep't 1980), (1980) UNJYB, 18 October 1979, p. 222 ("[T]he Pension Fund is an organ of the United Nations, subject to regulation by the General Assembly, and … its assets, although held separately from other United Nations property, are the property of that international organization").

supported by those servers, which makes them "property and assets" of the ICRC, and as such they are protected from hacking. Equally, where an IO can establish ownership or control over data that is stored on computer systems and networks operated by third parties, that data qualifies as "property and assets" of the IO and is protected from interference and specifically hacking.

Section 4 of the CPIUN provides that "[t]he archives of the United Nations, and in general all documents belonging to it or held by it, shall be inviolable wherever located". The term "archives" does not refer to historical documents only, but to "the entire collection of stored documents … including [the IO's] official records and correspondence".[30] In any event, Section 4 explains that "all documents" belonging to or held by IOs are inviolable. It is well established that, in the Digital Age, documents are inviolable irrespective of whether they are compiled physically or electronically.[31]

As Section 4 explains, archives and documents are inviolable when they "belong to" or are "held by" an IO. The latter term indicates that, even in the absence of ownership, archives and documents are protected when they are placed in an IO's "safekeeping".[32] In short, what is critical is that the IO exercises "control" over the archives and documents in question.[33] Moreover, the archives and documents of an IO are inviolable "wherever located". Consider, for example, a situation in which an IO stores data on servers in third States. It may be the case that the IO preserves its legal ownership of that data by concluding a contract with the actor who owns or controls the server. But even if ownership cannot be established, that data can be said to form part of the archives and documents of the IO where the organization exercises control over it, for example by being able to access, modify and delete the data or transfer it to another actor. Conversely, data does not form part of the archives and documents of an IO

30 Supreme Court of Canada, *World Bank Group*, above note 18, para. 73. The UN Secretary-General defines archives as "records to be permanently preserved for their administrative, fiscal, legal, historical or informational value": UN Secretariat, "Secretary-General's Bulletin: Record-Keeping and Management of United Nations Archives", ST/SGB/2007/5, 2007.

31 UK Supreme Court, *R (on the Application of Bancoult No. 3) v. Secretary of State for Foreign and Commonwealth Affairs*, [2018] UKSC 3, 8 February 2018, para. 68; Tallinn Manual 2.0, above note 21, p. 220; A. Reinisch and P. Bachmayer, above note 15, pp. 161–162; "Letter from the Assistant Secretary-General for Legal Affairs to the Minister Counsellor of a Permanent Mission to the United Nations", 5 September 2007. The UN Secretary-General defines documents as "any data or information, regardless of its form or medium, which is or has been electronically generated by, transmitted via, received by, processed by, or represented in an ICT resource": UN Secretariat, "Secretary-General's Bulletin: Use of Information and Communication Technology Resources and Data", ST/SGB/2004/15, 2004. "All records, including electronic records and e-mail records, created or received by a staff member in connection with or as a result of the official work of the United Nations, are the property of the United Nations": UN Secretariat, above note 30.

32 "[With regard to Section 4] we are thus talking about not only all the Organization's own documents but also those held by it, in other words those in its safekeeping": Leonardo Diaz-Gonzalez, *Fifth Report on Relations between States and International Organizations*, UN Doc. A/CN.4/432, 11 May 1990, p. 4. See also A. Reinisch and P. Bachmayer, above note 15, pp. 163–165.

33 "What is it that identifies a document as belonging to the archives or documents of the mission, as opposed to some other organ of the sending state? … The test is not their location, for they are protected 'wherever they may be'. It must necessarily be whether they are under the control of the mission's personnel": UK Supreme Court, *Bancoult No. 3*, above note 31, para. 68.

where the organization passes it to, or shares it with, another actor and in doing so relinquishes control over it.[34] In this context, the data can no longer be described as "belonging to" or "held by" the IO. However, this does not apply to MSs because when an IO shares data with them related to the functions of the organization, they act as organs of the IO and the data is still data of the organization. Otherwise, an IO would not be able to discharge its functions if relevant data were not protected when shared with its MSs.[35]

According to Section 10 of the CPIUN, "[t]he United Nations shall have the right to use codes and to despatch and receive its correspondence by courier or in bags, which shall have the same privileges and immunities as diplomatic couriers and bags". Electronic communications such as emails can be seen as correspondence analogous to courier dispatches and, where they contain attachments (for example, zip files), they can be analogized to diplomatic bags.[36] Under the VCDR, diplomatic bags must "bear visible external marks of their character".[37] In the cyber context, email addresses, subject lines and electronic signatures can be used to identify the communications of an IO.[38] Critically, diplomatic bags cannot be "opened or detained".[39] Airport security cannot therefore X-ray diplomatic bags because this would result in their contents being revealed. However, sniffer dogs can be used to search for drugs, explosives or other illicit items because such searches do not penetrate or otherwise reveal the contents of the bag. In the cyber context, sniffer software that can detect malicious emails is permitted but more intrusive software that reveals the content of emails is proscribed.[40]

We can thus conclude by saying that these privileges and immunities provide IOs with overlapping protection against hacking.

Privileges and immunities in headquarters agreements

IOs are almost always located within the territory of MSs, and this raises the possibility that the host State may interfere in the organization's work. In particular, host States have greater opportunity to hack the data of IOs because such organizations may use the cyber infrastructure located within the territory of host States to support their computer networks and systems and may use this infrastructure to connect and communicate with the outside world. IOs and host States thus conclude bilateral treaties – usually referred to as "headquarters agreements", "seat agreements" or "host State agreements" – to regulate their

34 *Ibid.*
35 Rosalyn Higgins, *Problems and Process: International Law and How We Use It*, Oxford University Press, Oxford, 1994, p. 93.
36 Eileen Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*, Oxford University Press, Oxford, 2016, p. 194.
37 Vienna Convention on Diplomatic Relations, 1961 (VCDR), Art. 27(4).
38 R. Buchan, above note 10, p. 87.
39 VCDR, Art. 27(3).
40 Won-Mog Choi, "Diplomatic and Consular Law in the Internet Age", *Singapore Year Book of International Law*, Vol. 10, 2006, p. 131.

relations and, in particular, maintain the IO's independence. These agreements cover different areas and usually award IOs the privileges and immunities they need to discharge their functions.[41]

Headquarters agreements tend to incorporate the privileges and immunities set out in the CPIUN.[42] At the same time, headquarters agreements can tailor the scope of the awarded privileges and immunities to the particular context of hosting an IO.[43] Since the CPIUN tends to act as the baseline for the privileges and immunities contained in headquarters agreements, and since (as explained in the previous section) these privileges and immunities protect IOs from hacking, headquarters agreements equally protect IOs from hacking by host States.

Privileges and immunities under customary international law

The preceding sections established the scope of the privileges and immunities enjoyed by IOs vis-à-vis their member States and host States. In this section, we consider whether NMSs should respect the privileges and immunities of IOs. Although NMSs are not bound by the privileges and immunities contained in agreements concluded by IOs or treaties to which they are not party,[44] the question arises as to whether these privileges and immunities (or at least certain privileges and immunities) have been absorbed into CIL and thus apply to the relationships between IOs and NMSs.

Commentators have cast doubt on whether IOs enjoy privileges and immunities under CIL due to the fact that IOs' privileges and immunities are invariably enshrined in treaties, meaning there is little scope for State practice and *opinio juris* to develop outside of this dense patchwork of conventional agreements.[45] Yet, the question of whether there is CIL on the privileges and immunities of IOs cannot be ignored because the treaties setting up IOs may be silent in this respect,[46] there may be no headquarters agreements, the existing agreements may not be comprehensive or enacted domestically, and above all because IOs are active participants in international life and interact with other actors, including NMSs.

41 A. Sam Muller, *International Organizations and Their Host States: Aspects of their Legal Relationship*, Brill, Leiden, 1995, p. 22.

42 *Ibid*., Chap. 6; Anthony J. Miller, "Privileges and Immunities of United Nations Officials", *International Organizations Law Review*, Vol. 4, No. 2, 2007, p. 170.

43 Pieter H. F. Bekker, *The Legal Position of Intergovernmental Organizations: A Functional Necessity Analysis of Their Legal Status and Immunities*, Martinus Nijhoff, Leiden, 1994, p. 136.

44 Vienna Convention on the Law of Treaties, 1969 (VCLT), Art. 34.

45 Michael Wood, "Do International Organizations Enjoy Immunity under Customary International Law?", in Niels M. Blokker and Nico J. Schrijver (ed.), *Immunity of International Organizations*, Brill, Leiden, 2015, p. 30; Edward Chukwuemeke Okeke, *Jurisdictional Immunities of States and International Organizations*, Oxford University Press, Oxford, 2018, p. 269. For a more nuanced approach, see Niels M. Blokker, "Jurisdictional Immunities of International Organisations – Origins, Fundamentals and Challenges", in Tom Ruys, Nicolas Angelet and Luca Ferro (eds), *The Cambridge Handbook of Immunities and International Law*, Cambridge University Press, Cambridge, 2019, pp. 194–197.

46 For example, the NATO Constitution and the Warsaw Treaty Pact Organization Charter.

In our opinion, a positive case can be made that certain privileges and immunities contained in the CPIUN have acquired the status of CIL – namely, those pertaining to premises, property, assets, archives, documents and correspondence.[47]

As a preliminary matter, we should recall that, according to the International Court of Justice (ICJ), for treaty provisions to pass into CIL, they must be "of a fundamentally norm-creating character such as could be regarded as forming the basis of a general rule of law". [48] When it comes to the CPIUN's provisions on privileges and immunities, there is little doubt that they are of a norm-creating character given that they require States Parties to respect and protect the inviolability of an IO's premises, property, assets, archives, documents and correspondence and do not permit any reservations or derogations. More critically, though, the CPIUN introduced the notion of functional privileges and immunities by shifting the approach away from sovereign privileges and immunities to privileges and immunities of non-sovereign entities – to wit, IOs. In this regard, at least certain provisions, such as those relating to premises, property, assets, archives, documents and correspondence, are generalizable as applying to all IOs because they enable such organizations to fulfil their functions without interference, in view also of the fact that IOs lack territory and the material and legal resources that States have at their disposal.

For CIL to arise, there must be a general practice and *opinio juris*.[49] The immediate question for the purposes of the present discussion, then, is whether there is a general practice accompanied by *opinio juris* in favour of the CPIUN's privileges and immunities provisions. One can say that where States become parties to a convention, the act of ratification evinces an intention to be bound by that treaty as a matter of treaty law, and from this, no State practice or *opinio juris* can be deduced to support the formation of CIL.[50] However, the ICJ has held that a treaty can be assimilated into CIL where there is "very widespread and representative participation in the convention" and its membership includes

47 "[T]he General Convention's provisions on jurisdictional immunity have been applied to other organizations and non-member states through the development of similar treaties and customary international law": Charles H. Brower II, "International Immunities: Some Dissident Views on the Role of Municipal Courts", *Virginia Journal of International Law*, Vol. 41, No. 1, 2001, p. 22. Amerasinghe explains that the CPIUN and the Specialized Agencies Convention reflect an "incipient customary law of international privileges and immunities" and that there is "a presumption that many of the privileges and immunities incorporated in the two general conventions are generally what are required for this purpose": C. F. Amerasinghe, above note 12, p. 346. See also Giorgio Gaja, "Jurisdictional Immunity of International Organizations", *Yearbook of the International Law Commission*, Vol. 2, Part 2, 2006, p. 202; Christian Dominicé, "L'immunité de juridiction et d'exécution des Organisations Internationales", *Recueil des Cours*, Vol. 187, 1984, pp. 174–177 ("Le probléme de la coutume"), 219–225 ("La question de la coutume"); James Crawford, *Brownlie's Principles of Public International Law*, Oxford University Press, Oxford, 2019, pp. 164–166.

48 ICJ, *North Sea Continental Shelf Cases*, Judgment, [1969] ICJ Rep. 3, 20 February 1969, para. 72.

49 Statute of the International Court of Justice, 1945, Art. 38(1)(b).

50 ICJ, *North Sea*, above note 48, para. 71; ICJ, *Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Judgment (Merits), [1986] ICJ Rep. 14, 17 June 1986, para. 184.

those States whose "interests" are "specially affected";[51] this approach has also been adopted by international courts,[52] commissions[53] and domestic courts.[54] In these circumstances, the widespread ratification of a treaty gives rise to a large body of State practice and signals the emergence of a communal *opinio juris*, and these combine to generate a parallel rule of CIL.[55] This approach to the formation of CIL is important in the context of the CPIUN given that the CPIUN has attracted widespread support within the international community, with 162 States having ratified it at the time of writing.[56]

The argument that provisions contained in widely ratified treaties are constitutive of CIL is even more compelling when those provisions are replicated

51 ICJ, *North Sea*, above note 48, para. 73. See also ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, [1996] ICJ Rep. 226, 8 July 1996, para. 82 (citing "the extent of the accession" to the Hague and Geneva treaties as confirming their CIL status). "The number of parties to a treaty may be an important factor in determining whether particular rules set forth therein reflect customary international law; treaties that have obtained near-universal acceptance may be seen as particularly indicative in this respect": ILC, *Draft Conclusions on Identification of Customary International Law, with Commentaries*, 2018, Conclusion 11, Commentary para. 3.

52 Special Court for Sierra Leone, *Prosecutor v. Sam Hinga Norman*, Case No. SCSL-2004-14-AR72(E), Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment), 31 May 2004, paras 17–20 (referring to the "huge acceptance, the highest acceptance of all international conventions" as indicating that the relevant provisions of the Convention on the Rights of the Child have passed into CIL).

53 "Certainly, there are important, modern authorities for the proposition that the Geneva Conventions of 1949 have largely become expressions of customary international law, and both Parties to this case agree. The mere fact that they have obtained nearly universal acceptance supports this conclusion": Eritrea–Ethiopia Claims Commission, *Partial Award: Prisoners of War, Ethiopia's Claim 4*, UNRIAA, Vol. 26, 1 July 2003, para. 31 (citations omitted).

54 "[A] treaty will only constitute sufficient proof of a norm of customary international law if an overwhelming majority of States have ratified the treaty, and those States uniformly and consistently act in accordance with its principles": District Court for the Eastern District of Virginia, *United States v. Hasan and Ors*, Decision on Motion to Dismiss, No. 2:10cr56, ILDC 1586 (US 2010), 29 October 2010, para. 87. The Court considered the definition of piracy in the UN Convention on the Law of the Sea to be reflective of CIL on the basis that 161 States had ratified it, which represented the "overwhelming majority": *ibid*., para. 89. See, generally, Cedric M. J. Ryngaert and Duco W. Hora Siccama, "Ascertaining Customary International Law: An Inquiry into the Methods Used by Domestic Courts", *Netherlands International Law Review*, Vol. 65, No. 1, 2018, pp. 6–10.

55 Crawford explains that there must be "a presumption of *opinio juris* from wide participation in a treaty, at least in normative terms": James Crawford, "Chance, Order, Change: The Course of International Law", *Recueil des Cours*, Vol. 365, 2013, para. 167. "[P]articipation in a treaty with a fundamentally norm-creating character (such as an IHL treaty) counts as practice capable of supporting the development of parallel rules of customary law": Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, Edward Elgar, Cheltenham, 2019, para. 4.40. See also Richard R. Baxter, "Multilateral Treaties as Evidence of Customary International Law", *British Yearbook of International Law*, Vol. 41, 1965–66, p. 275; Hugh Thirlway, *International Customary Law and Codification*, A. W. Sijthoff, Leiden, 1972, p. 89; Anthony D'Amato, *The Concept of Custom in International Law*, Cornell University Press, London and Ithaca, NY, 1971, p. 104.

56 It is interesting to note that in 1967 the UN Legal Counsel opined that "the standards and principles of the Convention have been so widely accepted that they have now become a part of the general international law governing the relations of States and the United Nations", and this was also correct in relation to NMSs; "Question of Privileges and Immunities of the United Nations, of Representatives of Member States and of Officials of the Organization: Statement made by the Legal Counsel at the 1016th Meeting of the Sixth Committee of the General Assembly on 6 December 1967", *United Nations Juridical Yearbook*, 1967, p. 314.

in successive treaties.[57] To explain, when a treaty provision is repeated in a series of subsequent conventions, this amounts to a general State practice and indicates the "gradual fusion of a communal *opinio juris*",[58] thereby furnishing the necessary ingredients to establish a rule of CIL. This is the case with the CPIUN. As explained previously, the CPIUN has been used as a template for many other treaties on privileges and immunities – in fact, the CPIUN's privileges and immunities provisions are usually repeated verbatim in most IOs' privileges and immunities treaties. This is a deliberate and conscious act which demonstrates both State practice and *opinio juris*.

Further evidence of the CIL status of the CPIUN's privileges and immunities provisions lies in the VCDR. The law on diplomatic privileges and immunities and the law on the privileges and immunities of IOs are closely related. The customary law of diplomatic privileges and immunities has a long history in international relations and has influenced the development of the law on the privileges and immunities of IOs, including the CPIUN.[59] Moreover, certain privileges and immunities contained in the 1946 CPIUN are replicated in the 1961 VCDR and, as we have seen, courts have frequently used the definitions of terms and concepts appearing in the VCDR to aid their interpretation of similar terms and concepts appearing in the CPIUN. Importantly, the ICJ has consistently found the VCDR to be reflective of CIL[60] and, as we explain in the next paragraph, certain IOs have been granted diplomatic privileges and immunities.

Headquarters agreements also provide evidence of the existence of CIL since certain agreements refer or allude to the customary law of privileges and immunities, such as the agreements concluded between Switzerland (as the host State) and many IOs. For example, Article 3 of the agreement with the International Labour Organization provides: "L'Organisation Internationale du Travail est au bénéfice de l'ensemble des immunités connues, en droit des gens,

57 "[I]n some cases it may be that frequent repetition in widely accepted treaties evinces a recognition by the international community as a whole that a rule is one of general, and not just particular, law": International Law Association, *Committee on Formation of Customary (General) International Law: Final Report*, 2000, Rule 25, Commentary para. 5. "The repetition in two or more codification conventions of the substance of the same norm may be an important element in establishing the existence of that norm as a customary rule of general international law": Institut de Droit International, *Problems Arising from a Succession of Codification Conventions on a Particular Subject*, Lisbon, 1995, Rule 12. "The fact that a rule is set forth in a number of treaties may, but does not necessarily, indicate that the treaty rule reflects a rule of customary international law": ILC, above note 51, Conclusion 11(2).

58 Yoram Dinstein, "The Interaction between Customary International Law and Treaties", *Recueil des Cours*, Vol. 322, 2006, pp. 299–300.

59 Alison Duxbury, "Intersections between Diplomatic Immunities and the Immunities of International Organizations", in Paul Behrens (ed.), *Diplomatic Law in a New Millennium*, Oxford University Press, Oxford, 2017.

60 ICJ, *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium)*, Judgment, [2002] ICJ Rep. 3, 14 February 2002, para. 52; ICJ, *Certain Questions of Mutual Assistance in Criminal Matters (Djibouti v. France)*, Judgment, [2008] ICJ Rep. 177, 4 June 2008, para. 174; ICJ, *United States Diplomatic and Consular Staff in Tehran*, Judgment, [1980] ICJ Rep. 3, 24 May 1980, paras 62, 69.

sous le nom d'immunités diplomatiques";[61] Article 2 of the agreement with the European Free Trade Association explains: "L'Association jouit des immunités et privilèges habituellement reconnus aux organisations internationales";[62] Article 2 of the agreement with the European Organization for Nuclear Research provides: "The Organization shall enjoy the immunities and privileges usually granted to international organizations to the extent required for the fulfilment of their tasks";[63] and Article 2 of the agreement with the World Health Organization explains: "L'Organisation Mondiale de la Santé est au bénéfice de l'ensemble des immunités connues, en droit des gens, sous le nom d'immunités diplomatiques."[64]

How national courts deal with the privileges and immunities of IOs can provide evidence of the existence of CIL. For example, in *A. S. v. Iran–United States Claims Tribunal*, the Dutch Supreme Court held that, in the absence of an agreement on privileges and immunities, "it follows from unwritten international law that an international organization is entitled to the privilege of immunity from jurisdiction on the same footing as generally provided for in the treaties referred to above [namely, headquarters agreements and privileges and immunities conventions]".[65] In another case, an Israeli court granted absolute immunity to the European Commission even in relation to commercial matters because "it is not a sovereign state but an international organisation with certain goals" to which the impugned act fell.[66]

What we can conclude from the preceding discussion is that certain provisions of the CPIUN – specifically, those on the inviolability of premises, property, assets, archives, documents and correspondence – have transitioned into CIL.[67] This is because they have been reaffirmed by State practice and *opinio juris*, as evinced by their formulation in relevant conventions. More importantly, they are supported by the practice and *opinio juris* of IOs. Although views as to whether IOs can contribute to the creation of CIL may differ, we subscribe to the International Law Commission's (ILC) view that they can do so in certain cases, such as when the subject falls within an IO's mandate and/or the rule is addressed to IOs.[68] Privileges

61 Accord du 11 Mars 1946 entre le Conseil Fédéral Suisse et l'Organisation Internationale du Travail pour régler le Statut Juridique de cette Organisation en Suisse, available at: www.fedlex.admin.ch/eli/cc/1956/1103_1182_1194/fr.

62 Accord entre le Conseil Fédéral Suisse et l'Association Européenne de Libre-échange pour déterminer le Statut Juridique de cette Association en Suisse, available at: www.fedlex.admin.ch/eli/cc/1961/749_763_779/fr.

63 European Organization for Nuclear Research, *Headquarters Agreement*, CERN/115 Rev. 2, 11 February 1955, available at: https://cds.cern.ch/record/21737/files/CM-P00074863-e.pdf.

64 Accord entre le Conseil Fédéral Suisse et l'Organisation Mondiale de la Santé, pour régler le Statut Juridique de cette Organisation en Suisse Conclu le 21 août 1948, available at: www.fedlex.admin.ch/eli/cc/1956/1120_1198_1210/fr.

65 Supreme Court of the Netherlands, *A. S. v. Iran–United States Claims Tribunal*, RvdW (1986) No. 20, NJ (1986) No. 438, 20 December 1985, *Netherlands Yearbook of International Law*, Vol. 18, 1987, p. 360.

66 Haggai Carmon, "A Jerusalem Court Ruling: The European Commission is Immune to a Commercial Lawsuit", *Diplomatic/Consular Law and Sovereign Immunity in Israel and Worldwide*, available at: http://diplomaticlaw.com/blog/?p=100.

67 J. Crawford, above note 47, pp. 164–166.

68 ILC, above note 51, Conclusion 4(2), Commentary paras 5, 6. See also Kristina Daugirdas, "International Organizations and the Creation of Customary International Law", *European Journal of International Law*, Vol. 31, No. 1, 2020, p. 201; C. Dominicé, above note 47, pp. 220–225.

and immunities is indeed an area where IOs engage in practice and express their *opinio juris*. As we have noted, this is because the privileges and immunities conventions and the headquarters agreements that replicate the CPIUN are negotiated and signed by the relevant IO as an international legal person.

Moving forward, another ground on which the CIL of privileges and immunities can be established is the international legal personality of IOs. Privileges and immunities are attendant to and give effect to the distinct legal personality of IOs; they therefore constitute part of the bundle of customary law rights attached to the legal personality of IOs.[69]

This raises the question of when IOs enjoy legal personality under international law, the answer to which depends on whether legal personality is established subjectively or objectively. The subjective approach awards legal personality to IOs on the basis of the express or implied intention of their MSs. For example, MSs can explicitly endow the IO with legal personality in its constitutive treaty, or such personality can be inferred from the terms of the treaty. Insofar as NMSs are concerned, if they recognize (either explicitly or through acquiescence) an IO's legal personality, they also accept the attendant CIL privileges and immunities. Conversely, if they do not recognize the legal personality of an IO, they are not under any obligation to respect its privileges and immunities.

However, the subjective approach is not the dominant one. Rather, the prevailing view is that the legal personality of IOs is objectively established as a matter of international law.[70] According to this approach, IOs are bestowed with legal personality if they exhibit certain attributes, such as organs, powers and functions. This was how the ICJ established the legal personality of the UN in the absence of a specific provision in the Charter.[71] The significance of an IO's objective legal personality is that it operates *erga omnes* and is therefore opposable to NMSs.[72]

69 "[T]he privileges and immunities of an international organization derive from its legal status as an international person": E. C. Okeke, above note 45, p. 253. See also Fernando Lusa Bordin, "To What Immunities are International Organizations Entitled under General International Law? Thoughts on *Jam v IFC* and the 'Default Rules' of IO Immunity", *Questions in International Law*, Vol. 72, No. 1, 2020, p. 5. Italian case law has derived immunities from the legal personality of an IO. See Italian Court of Cassation, *Christiani v. ILAI*, Judgment No. 5819/1985, *Rivista di Diritto Internazionale*, 1986, p. 149. Dominicé takes the view that an IO with legal personality and whose MSs have granted it jurisdictional immunities as a matter of customary law enjoys the same immunities vis-à-vis NMSs (third States), but this may not be the case if the IO does not enjoy immunities vis-à-vis its MSs; C. Dominicé, above note 47, pp. 222–224.

70 Finn Seyersted, *Objective International Personality of Intergovernmental Organisations: Do Their Capacities Really Depend upon their Constitutions?*, Copenhagen, 1963, pp. 9–10; C. W. Jenks, above note 12, p. 34; Philippe Sands and Pierre Klein, *Bowett's Law of International Institutions*, Sweet and Maxwell, London, 2009, p. 490; Nigel D. White, *The Law of International Organisations*, Manchester University Press, Manchester, 2017, pp. 101–120.

71 ICJ, *Reparation for Injuries Suffered in the Service of the United Nations*, Advisory Opinion, [1949] ICJ Rep. 174, 11 April 1949, pp. 177–185. See also DARIO, above note 11, Art. 2, Commentary para. 9.

72 "There are those who take the view that the international legal personality of an organization is opposable only to those who have 'recognised' the organization, in the sense of being a member of the organization or engaging in some transaction with it, or granting privileges to it. But this is to ignore the objective legal reality of international personality. If the attributes are there, personality exists. It is not a matter of recognition. It is a matter of objective reality": R. Higgins, above note 35, pp. 47–48. "[T]he personality

Accordingly, NMSs should respect the privileges and immunities that are attendant to an IO's legal personality.[73]

To summarize, in this section we have argued that the privileges and immunities found in constitutive treaties, conventions and headquarters agreements protect IOs from hacking and that these privileges and immunities can be extended to NMSs because they are established in CIL and attach to the legal personality of IOs.

The principle of good faith: Its application to international organizations and hacking

In this section we discuss the application of the principle of good faith (GF) to the relations between IOs, MSs and NMSs, and consider how GF protects IOs from hacking. This section will explain the legal status of GF, establish its applicability to the relations between IOs, MSs (including host States) and NMSs, identify its particular postulates, and explain how it protects IOs from hacking.

The legal status of good faith

GF is a general principle of international law[74] whose modern formulation derives from the Roman concept of *bona fides*, which refers to trustworthiness, conscientiousness and honourable conduct.[75] In fact, GF is a fundamental principle of international law[76] because it upholds the integrity and effectiveness

of international organizations is in fact objective, which means that it is opposable to non-members and that non-members are bound to accept that organization as a separate legal person": Dapo Akande, "International Organizations", in Malcolm Evans (ed.), *International Law*, Oxford University Press, Oxford, 2018, p. 233. The United States claims that the objective legal personality of an IO depends on the size of its membership: "An international organization with substantial membership is a person in international law even in relation to states not members of the organization. However, a state does not have to recognize the legal personality of an organization of which it is not a member, which has few members, or which is regional in scope in a region to which the state does not belong." "Restatement (Third) of Foreign Relations Law of the United States", American Law Institute, 1987, Section 223, Comment (e). However, as Amerasinghe explains, once the legal personality of an IO is objectively established, there is no need to inquire into the size of its membership: C. F. Amerasinghe, above note 12, pp. 86–91.

73 J. Crawford, above note 47, p. 163; F. L. Bordin, above note 69, pp. 8–15; N. D. White, above note 70, p. 117.

74 Statute of the International Court of Justice, 1945, Art. 38(1)(c). See also ICJ, *Land and Maritime Boundary between Cameroon and Nigeria*, Judgment (Preliminary Objections), [1998] ICJ Rep. 275, 11 June 1998, para. 38; ICJ, *Certain Norwegian Loans*, [1957] ICJ Rep. 9, 6 July 1957, p. 53 (Separate Opinion of Judge Lauterpacht) ("Unquestionably, the obligation to act in accordance with good faith, being a general principle of law, is also part of international law"); Bin Cheng, *General Principles of Law as Applied by International Courts and Tribunals*, Cambridge University Press, Cambridge, 1953, Part II; Michel Virally, "Good Faith in Public International Law", *American Journal of International Law*, Vol. 77, No. 1, 1983, p. 130; Robert Kolb, *Good Faith in International Law*, Hart, Oxford, 2017. For a more critical approach, see Elisabeth Zoller, *La bonne foi en droit international public*, A. Pédone, Paris, 1977.

75 John F. O'Connor, *Good Faith in International Law*, Dartmouth, Aldershot, 1991, pp. 18–19, 124.

76 According to Schwarzenberger, GF is "a fundamental principle which can be eradicated from international law only at the price of the destruction of international law itself [and] forms necessarily

of the international legal order by fostering respect for the law as well as trust and confidence in legal relations.[77] GF thus ensures the stability and predictability of international legal relations, which is critical in an order characterized by voluntarism, weak institutional enforcement mechanisms, and value and power differentiation. It is for this reason that GF informs all international legal relations, including those established by IOs.[78]

Although GF is sometimes referred to as a CIL rule,[79] the ICJ and other judicial bodies do not always differentiate between customary rules and general principles but instead view general principles as the formulation of fundamental and general rules. In fact, they place CIL and general principles under the umbrella of general international law.[80]

That said, the classification of GF as a general principle is in our opinion the most appropriate because it corresponds to its general content, acceptance and binding effect. The legal implications that flow from the classification of GF as a general principle are as follows. First, GF has independent legal standing and binds all international legal persons.[81] It is also legally consequential in that it produces legal consequences when applied to particular situations.[82] In this regard, there are similarities between GF as a general principle and customary law because they both bind all international legal persons (with the exception of

part of the international public order. This consideration alone would suffice to qualify good faith as one of the fundamental principles of international law"; Georg Schwarzenberger, "The Fundamental Principles of International Law", *Recueil des Cours*, Vol. 87, 1955, p. 326. See also B. Cheng, above note 74, p. 105; ILC, *First Report on General Principles of Law*, UN Doc. A/CN.4/732, 2019, para. 154.

77 ICJ, *Nuclear Tests (Australia and New Zealand v. France)*, Judgment (Questions of Jurisdiction and/or Admissibility), [1974] ICJ Rep. 457, 20 December 1974, para. 46; Guillaume Futhazar and Anne Peters, "Good Faith", in Jorge E Viñuales (ed.), *The UN Friendly Relations Declaration at 50: An Assessment of the Fundamental Principles of International Law*, Cambridge University Press, Cambridge, 2020, p. 191.

78 "Good faith is a supreme principle, which governs legal relations in all of their aspects and content": International Centre for Settlement of Investment Disputes, *Inceysa Vallisoletana s.l. v. Republic of El Salvador*, ICSID Case No. ARB/03/26, Award of 2 August 2006, para. 230. See also ICJ, *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)*, Jurisdiction of the Court and Admissibility of the Application, [1984] ICJ Rep. 392, 29 November 1984, para. 60; ILC, above note 76, para. 161.

79 Permanent Court of International Justice, *Case Concerning Certain German Interests in Polish Upper Silesia*, Judgment No. 7, [1926] PCIJ Series A, 25 May 1926, pp. 1, 39–40; Court of First Instance of the European Communities, *Opel Austria GmbH v. Council*, Case No. T-115/94, [1997] ECR II-39, 22 January 1997, paras 24, 89–90.

80 ICJ, *Delimitation of Maritime Boundary in Gulf of Maine Area*, Judgment, [1984] ICJ Rep. 246, 12 October 1984, para. 79; World Trade Organization, Appellate Body, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, 12 October 1998, para. 158; ILC, above note 76, paras 142–162.

81 ICJ, *Reparation for Injuries*, above note 71 (where the ICJ viewed the UN (as an IO) and States as "two political entities, equal in law, similar in form, and both the direct subjects of international law": pp. 177–179). Also see ICJ, *Interpretation of the Agreement of 25 March 1951 between the WHO and Egypt*, Advisory Opinion, [1980] ICJ Rep. 73, 20 December 1980, para. 37 ("International organizations are subjects of international law, and, as such, are bound by any obligations incumbent upon them under general rules of international law").

82 "It is clear to this Tribunal that the investment made by Inceysa in the territory of El Salvador, which gave rise to the present dispute, was made in violation of the principle of good faith": International Centre for Settlement of Investment Disputes, *Inceysa Vallisoletana s.l.*, above note 78, para. 234.

persistent objectors in the case of custom[83]) and both produce legal consequences. Second, as a general principle GF contains a cluster of more specific postulates that give effect to its normative content, as will be seen in the subsection below on "The Content of Good Faith and Its Application to Hacking". Third, certain of these postulates have acquired the status of independent rules, but this does not mean that GF has become otiose. GF remains as the background principle that assists in the application and interpretation of these specific rules, but more critically, it applies directly to fill any legal gaps that arise.[84] Fourth, the application of GF as a general principle to a particular set of circumstances and legal relations requires a certain contextualization. This is indeed one of the main differences between general principles and rules, with the latter applying in an "all-or-nothing" fashion.[85] In relation to IOs, it means that the content of GF may be thicker or thinner depending on the nature of the IO,[86] or whether GF applies to the relations between IOs and their MSs, host States, or NMSs, as we shall see later.

The application of good faith to the relations between international organizations and member States

As we have noted, IOs are created by States to pursue common goals, and for this reason MSs assume certain procedural and substantive obligations towards each other and towards the organization. However, and notwithstanding certain exceptions,[87] IOs do not have their own binding mechanisms for interpreting and enforcing these obligations. Moreover, IOs, even those with legal personality, are dependent on States for institutional and material resources. The relationship between IOs and their MSs is therefore complex: it is a relationship of interdependence and mutual interactions which can be simultaneously vertical and horizontal because MSs remain sovereign and independent legal persons even within the IO and because they continue to exist and operate outside the IO and sometimes in competition with it.

In such a context, the role of GF is critical in ensuring the integrity, viability and effectiveness of the political and legal order established by the IO. GF sets out the modalities according to which obligations and interactions are to be performed in order for the IO to function and attain its objectives, while also maintaining its integrity and independence as a separate legal person.

83 ICJ, *North Sea*, above note 48, p. 44; ICJ, *Fisheries Case (United Kingdom v. Norway)* (Merits), [1951] ICJ Rep. 116, 18 December 1951, p. 131.

84 M. Virally, above note 74, p. 134: "[G]ood faith is often hidden by the more precise rules it has generated (e.g. *pacta sunt servanda*), so that it becomes no longer necessary to rely upon it expressly for ordinary practical purposes. But even in such instances, general principles retain their full value as the *ratio legis* to which one may profitably turn in difficult cases." See also Alain Pellet and Daniel Müller, "Article 38", in Andreas Zimmermann and Christian J. Tams (eds.), *The Statute of the International Court of Justice: A Commentary*, Oxford University Press, Oxford, 2019, para. 297.

85 Ronald Dworkin, *Taking Rights Seriously*, Duckworth, London, 1978, Chaps 2, 3; Joseph Raz, "Legal Principles and the Limits of Law", *Yale Law Journal*, Vol. 81, No. 5, 1972, p. 823.

86 In relation to the EU, see Court of Justice of the European Union, *Greece v. Commission*, Case No. C-203/07 P, [2008] ECR I-8161, 2008, para. 83 (Opinion of Advocate-General Mazák).

87 For example, the EU or Section 30 of the CPIUN.

It is for this reason that the principle of GF has been specifically included in the constitutive treaties of certain IOs, such as in Article 2(2) of the UN Charter[88] and Article 4(3) of the Treaty on European Union.[89] However, even in the absence of a specific rule, GF will still apply because, as has been explained, IOs and MSs as legal persons are bound by general principles of international law and because GF is part and parcel of the law of treaties, which governs the IO's constitutive instrument. [90]

Good faith in the relations between international organizations and host States

IOs and host States sign headquarters agreements which, as we have seen, define among other issues the privileges and immunities enjoyed by the organization. GF as part of the law of treaties thus governs the relations between an IO and the host State as formulated in the headquarters agreement. However, headquarters agreements or constitutive treaties do not regulate the whole spectrum of relations between IOs and host States, as the *WHO/Egypt* Advisory Opinion demonstrates. The question put to the ICJ was: "What are the legal principles and rules applicable to the question under what conditions and in accordance with what modalities a transfer of the Regional Office from Egypt may be effected?"[91] This issue is not covered by the headquarters agreement or the WHO constitutive treaty.

In such cases, GF applies directly to fill the gap by taking into consideration the special character of the relations between IOs and host States. This refers to the fact that the host State can facilitate or hinder the functioning of the IO more easily than any other MS because it provides the physical location and the resources that enable the IO to function as an independent legal person and carry out its activities.[92] It is for this reason that in the *WHO/Egypt* Advisory Opinion the ICJ stressed the importance of GF in the relations between IOs and host States.[93] The Court derived the principle of GF from "general international law", thus going beyond the treaty-based obligations of the parties. The Court examined a considerable number of headquarters agreements in order to establish how the relations between IOs and host States should be regulated, but also what GF

88 See Article 2(2) of the UN Charter in Bruno Simma, Daniel-Erasmus Khan, Georg Nolte and Andreas Paulus (eds), *The Charter of the United Nations: A Commentary*, Oxford University Press, Oxford, 2012. See also UNGA Res. 2625 (XXV), "Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations", 24 October 1970, Principle 4.

89 See also Articles 13(2) and 24(3) of the Treaty on European Union. See, generally, Geert De Baere and Timothy Roes, "EU Loyalty as Good Faith", *International and Comparative Law Quarterly*, Vol. 64, No. 4, 2015.

90 See Articles 26 and 31 of the VCLT and of the Vienna Convention on the Law of Treaties between States and International Organizations or between International Organizations, 1986.

91 ICJ, *WHO/Egypt*, above note 81, para. 48.

92 See *ibid.*, pp. 155–162 (Separate Opinion of Judge Ago).

93 The ICJ explained that the very essence of these relations "is a body of mutual obligations of co-operation and good faith": *ibid.*, para. 43. See also *ibid.*, p. 158 (Separate Opinion of Judge Ago).

requires in such cases.[94] What the Court did, in other words, was to apply GF to the relations between IOs and host States as general international law and to contextualize its application to the specific circumstances of the case concerning the removal of offices. This led the Court to identify the more specific GF obligations that the host State or any host State will have in this respect.

Good faith in the relations between international organizations and non-member States

IOs and NMSs interact in many different ways, but the fact that they may have no conventional relations or that their conventional relations do not cover all aspects of their interactions does not mean that they interact in a legal void. Instead, general principles (and CIL) provide the default legal framework that governs their relations.

The *Reparation for Injuries* Advisory Opinion is again instructive in this regard because the ICJ applied a general principle of law to the relations between the UN and an NMS. The ICJ opined that the right of the UN as an IO to claim reparations for breaches of international law from an NMS (Israel, in this instance) and the corresponding duty of an NMS to provide reparations derive from the general principle to make reparations, which the Permanent Court of International Justice had established in a previous Advisory Opinion[95] and when read in conjunction with the objective legal personality of the UN.[96]

It thus follows that GF as a general principle applies to any conventional legal relations between NMSs and IOs as part of the law of treaties, but also to relations arising from other general principles of international law and/or CIL – for example, the customary law of privileges and immunities or the principle of providing reparations. Beyond this, GF governs all other interactions between IOs and NMSs, giving rise to more specific legal postulates relative to the nature of their interactions, as will be seen in the next section.

The content of good faith and its application to hacking

Having established the applicability of GF to the relations between IOs, MSs, host States and NMSs, we will now consider GF's content in order to determine whether hacking breaches this principle. Before doing this, it is important to recall three points made earlier. The first is that, even if certain obligations emanating from GF have acquired independent legal standing, GF remains their normative source and GF continues to maintain its own independent legal standing and force. The second is that the content and scope of GF may differ depending on the nature of the legal relations to which it applies. The third point

94 *Ibid.*, paras 46, 48.

95 Permanent Court of International Justice, *Competence of the International Labour Organization to Regulate, Incidentally, the Personal Work of the Employer*, Advisory Opinion No. 13, [1926] PCIJ Series B, 23 July 1926, p. 18.

96 ICJ, *Reparation for Injuries*, above note 71, pp. 177–179, 183–185.

is that GF embodies a network of more specific substantive and procedural obligations; some of these have a negative dimension insofar as they require States to abstain from certain conduct, while others have a positive dimension insofar as they require certain conduct.

Turning now to the bundle of obligations flowing from GF, the first is that of *pacta sunt servanda*. *Pacta sunt servanda* is part and parcel of the law of treaties,[97] and it is accepted that it applies to all international legal obligations, including those arising from general principles of international law and CIL.[98]

GF is the normative source of *pacta sunt servanda*.[99] If the *pacta sunt servanda* rule were to be seen in isolation, it would be a circular and empty rule because it does not add anything new to the international law maxim that consent is the basis of legal obligations. That said, consent alone cannot guarantee the durability of obligations or their effective performance because it can be withdrawn at any time. That is why the *pacta sunt servanda* rule should be considered within its normative source – namely, the principle of GF – which requires States not only to comply with the obligations to which they have consented but also to carry out fully the terms of these obligations. This is also the reason why treaties and indeed constitutive treaties of IOs contain specific rules on GF or rules aligning *pacta sunt servanda* to GF, because simply consenting to a treaty establishing an IO is not sufficient to make it a functioning IO.

Insofar as hacking is concerned, hacking by MSs (including host States) breaches the *pacta sunt servanda* rule as it applies to their conventional obligations – for example, their obligation to respect the IO's privileges and immunities contained in special agreements or the constitutive treaty as discussed in the above section on "International Organizations and their Privileges and Immunities" – unless of course the particular act of hacking is justified under international law.[100] To the extent that certain privileges and immunities have acquired CIL status as argued in the above subsection on "Privileges and Immunities under Customary International Law", GF also covers these

97 For example, see VCLT, Art. 26. See also ICJ, *Nuclear Tests*, above note 77, para. 46 ("the very rule of *pacta sunt servanda* in the law of treaties is based on good faith"); ICJ, *Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia)*, Request for the Indication of Provisional Measures, [2014] ICJ Rep. 147, 3 March 2014, para. 44 ("Once a State has made a commitment concerning its conduct, its good faith in complying with that commitment is to be presumed"); J. F. O'Connor, above note 75; John B. Whitton, "La règle 'pacta sunt servanda'", *Recueil des Cours*, Vol. 49, 1934, pp. 151–216.

98 The UN General Assembly's Friendly Relations Declaration (UNGA Res. 2625 (XXV), above note 88), for example, affirms that good faith applies to all international obligations. In *Nuclear Tests* (above note 77), the ICJ explained that GF governs legal obligations "whatever their source" (para. 46) and then grounded the binding effect of unilateral obligations on GF (para. 49). See, further, Hersch Lauterpacht, "The Nature of International Law and General Jurisprudence", *Economica*, Vol. 37, 1932, p. 315.

99 B. Cheng, above note 74, pp. 105–162; G. Futhazar and A. Peters, above note 77, p. 195.

100 For that, see DARIO, above note 11, mainly Chap. V; ILC, *Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, 2001 (ARSIWA), mainly Chap. V. Good faith has not yet been recognized as a *jus cogens* norm the wrongfulness of whose violation cannot be precluded: see Article 26 of both DARIO and ARSIWA. The view that it is a *jus cogens* norm has been put forward by Robert Kolb, *Peremptory International Law – Jus Cogens: A General Inventory*, Hart, Oxford, 2015, pp. 56–58.

obligations, which in turn makes hacking by MSs and also NMSs a breach of this rule.

Second, GF entails a duty of cooperation between and among MSs and IOs in order to promote and attain the agreed objectives as they are formulated in the IOs' constitutive instruments, but also in other agreements.[101] This is not just a procedural obligation but also a substantive one, although it does not mandate a certain result. It requires MSs to communicate and consult with each other and with the IO in an honest and meaningful way, maintain good working relations, support and assist the IO, provide the required resources, refrain from withholding or disrupting services, reconcile interests, and find solutions to problems. In short, MSs must interact with each other and with the IO in such a way as to facilitate the functioning of the IO and the attainment of its objectives, and, at a minimum, must not actively or consciously hinder the work of the IO.[102] This obligation also extends to the settlement of disputes, particularly in the absence of dispute settlement mechanisms.

Evidently, the obligation to cooperate as a postulate of GF is most pertinent in the relations between IOs and their MSs (and especially the host State). This is further reinforced by the limitations imposed on the power of MSs to take countermeasures against an IO of which they are members.[103] More specifically, MSs can take countermeasures only if no other appropriate means of inducing compliance are available, which highlights the importance of the duty to cooperate.

Hacking by MSs breaches the duty to cooperate with the IO based on the free and confidential exchange of information, meaningful consultations, trust and honesty.[104] Hacking also damages the working relationship between the MS and the IO and disrupts the functioning of the IO. With regard to NMSs, the degree to which the duty to cooperate applies depends on the nature and scope of their relations with the IO; for example, if a dispute arises between an NMS and an IO involving hacking, they should cooperate in order to settle it peacefully.

Third, GF entails a duty to respect the legal personality of the IO. Respecting the personality of an IO encompasses a duty to abstain from practices, behaviours and acts inside or outside the IO that undermine the IO as a legal person. Among others, it includes a duty to respect the IO's capacity to hold meetings and make decisions; discuss issues; consult with MSs; collect, store and share information; and communicate freely within and among organs and

101 ICJ, *WHO/Egypt*, above note 81, paras 43, 48–49. See also ICJ, *Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights*, Advisory Opinion, [1999] ICJ Rep. 62, 29 April 1999, pp. 109–110 (Separate Opinion of Judge Rezek). See also R. Kolb, above note 74, pp. 162–163.

102 It can be argued that the use of privileges and immunities, as discussed earlier, is one way of achieving this purpose. The broader question is whether, in the absence of a specific agreement or customary law, GF can justify the granting of privileges and immunities or justify extending them if they have already been provided. In relation to host States, see R. Higgins, above note 35, pp. 90–91 (but for a more cautious approach, see C. F. Amerasinghe, above note 12, p. 347).

103 DARIO, above note 11, Art. 52.

104 "US Diplomats Spied on UN Leadership", *The Guardian*, 28 November 2010, available at: www.theguardian.com/world/2010/nov/28/us-embassy-cables-spying-un.

between organs and MSs in order to make decisions or implement tasks. Where an MS (including a host State) hacks without legal justification into an IO's computer networks and systems in order to acquire data or hacks data owned by the IO residing on servers operated by other actors, such conduct violates the GF obligation to respect the personality of the IO. It undermines the IO's operational autonomy in decision-making, supplants its decision to keep that information confidential, impacts on its ability to make independent decisions to the extent that its decisions can be manipulated, and, above all, affects its ability to dispose of its resources, competences and functions as it chooses, which is the essence of independent legal personality. For example, responding to Russia's attempted hack of the OPCW, and bearing in mind that Russia is a State party to the OPCW, the Dutch defence minister Ank Bijleveld explained that "[a]ny incident in which the integrity of international organisations is undermined is unacceptable".[105]

The importance of this GF postulate can also be demonstrated by the limitations imposed on the ability of MSs to take countermeasures against IOs. Suppose, for example, that an MS hacks data covered by privileges and immunities or exfiltrates confidential information but claims that the act was a lawful countermeasure because it was in response to a previous violation by the IO of an obligation owed to that State. According to the *Draft Articles on the Responsibility of International Organizations* (DARIO), MSs can take countermeasures against an IO only if it is in accordance with the "rules of the organization" in the sense that these rules allow countermeasures for breaches of the external and/or internal obligations owed by the IO to its MSs.[106] We are not aware of any such provision in the constitutive treaties of IOs, but what is important to stress for our purposes is that this approach to countermeasures deviates significantly from the general international law approach whereby States can take countermeasures against any violation of international law even if this is not specifically provided for in a particular instrument. The rationale behind such a limitation is to preserve the autonomy and independence of IOs and their ability to fulfil their functions against any pressure from MSs in the form of (or under the pretext of) countermeasures.

The GF obligation to respect the legal personality of IOs also applies to NMSs, since IOs enjoy objective legal personality. Consequently, NMSs should refrain from activities and behaviours that undermine the IO as an independent and autonomous legal person. Hacking which is not justified under international law constitutes such an activity.

Fourth, GF entails a duty of due regard to the rights, decisions, interests and legitimate expectations of the IO. This relates to and reinforces other duties such as *pacta sunt servanda*, respect of personality, and cooperation. It is both a procedural and substantive duty. How it will be fulfilled depends on the circumstances, and there is no particular course of conduct that should be adopted. The *Chagos Marine Protected Area* tribunal held that it requires a balancing of the rights and interests of the parties by also taking into consideration the importance of the

105 "Netherlands Defence Intelligence and Security Service disrupts Russian Cyber Operation", above note 5.
106 DARIO, above note 11, Art. 52; see also Arts 51–54.

impairment of rights.[107] The duty of due regard applies to MSs when they act within or outside the IO, and also applies to NMSs when they interact with the IO. Hacking by MSs and NMSs breaches the GF obligation of due regard if it is not the outcome of a conscious balancing of the rights and interests of the hacking State with those of the IO and no attempt to communicate or consult has been made.[108]

Fifth, GF entails a duty of loyalty to the IO. This relates to and reinforces all the preceding duties; for example, it reinforces the obligation to abide by mutual obligations, comply with the decisions of the IO, give due regard even to non-binding decisions,[109] cooperate with the IO, and respect its personality. The duty of loyalty serves the interests of an IO by imposing constraints on the exercise of MS powers within or outside the IO in order to ensure its effective functioning and independent standing. This duty also applies to the servants of IOs,[110] but does not apply to NMSs. Hacking by MSs that is not justified under international law breaches the duty of loyalty by not respecting the IO's processes and decisions and by reneging on any specific obligation that MSs have to respect the confidentiality or integrity of data belonging to an IO.

Sixth, GF entails an obligation on the part of MSs not to abuse their rights, powers and discretion in order to gain an advantage over the IO.[111] This duty also relates to the duties to respect the personality of the IO, to cooperate with it, and to respect the allocation of its powers. Hacking by an MS which has no valid legal justification constitutes the use by that MS of its power and position within the IO to serve its own interests and not those of the IO.

To conclude, we can say that hacking by MSs, host States and NMSs can breach a number of legal postulates flowing from GF, although the scope of the violation may differ depending on the nature of the relations between the IO and the State that committed the hacking.

Hacking and the principle of State sovereignty

In this section we consider whether the hacking of an IO by an MS or NMS breaches the sovereignty of the host State or the sovereignty of the State on whose cyber infrastructure the IO's data is located. This question is relevant because an IO's computer networks and systems are necessarily supported by cyber infrastructure that is physically located within the territory of a State, which may be either the

107 Permanent Court of Arbitration, *The Chagos Marine Protected Area Arbitration (Mauritius v. U.K.)*, Award of 18 March 2015, paras 519, 534.

108 *Ibid*., paras 530–535.

109 ICJ, *Voting Procedure on Questions relating to Reports and Petitions concerning the Territory of South West Africa*, Advisory Opinion, [1955] ICJ Rep. 76, 7 June 1955, pp. 118–119 (Separate Opinion of Judge Lauterpacht).

110 See UN Charter, Arts 100, 101.

111 ICJ, *Conditions of Admission of a State to Membership in the United Nations*, Advisory Opinion, [1948] ICJ Rep. 57, 28 May 1948, pp. 62–63. See also *ibid*., Dissenting Opinion of Judges Basdevant, Winiarski, Sir Arnold McNair and Read, paras 20, 83, 91, and Individual Opinion of Judge Alvarez, p. 71; World Trade Organization, *Shrimp Products*, above note 80, para. 158; B. Cheng, above note 74, p. 121; Alexandre Kiss, "Abuse of Rights", *Max Planck Encyclopedia of International Law*, 2006.

territory of the host State or a third State if the IO transmits its data through, or stores its data on, cyber infrastructure located within that State's territory. In order to answer this question, we first need to explain the status, content and scope of the principle of State sovereignty

It is nowadays well established that the principle of State sovereignty applies to cyberspace.[112] According to this principle, a State is entitled to exercise its sovereign rights over its territory and people free from interference.[113] In relation to cyberspace, sovereignty covers all cyber infrastructure located within a State's territory and under its jurisdiction regardless of whether it is publicly or privately owned or operated, and in addition, it encompasses the computer networks and systems supported by that infrastructure.[114]

That said, States are currently divided as to when cyber operations breach the principle of State sovereignty. Certain States take the view that cyber operations breach this principle when there is unauthorized intrusion into another State's sovereign cyber domain, while others argue that such operations are unlawful only when they cross a *de minimis* threshold – namely, when they cause damage to, or at least interfere with, the functionality of systems, or when they interfere with governmental functions.[115] This is an issue that can be resolved only through State practice and *opinio juris*, although in our opinion any unauthorized intrusion into a State's cyber infrastructure (such as hacking) would constitute a breach of its sovereignty.[116] We also reject the view that hacking falls beyond the prohibitive scope of the principle of State sovereignty because of its frequency.[117] The present article is not the place to enter this complex debate, but as one of the authors has written elsewhere, hacking is a weak contender for a CIL exception because it is often unaccompanied by the requisite *opinio juris*.[118]

112 See, for example, Switzerland, *Position Paper on the Application of International Law in Cyberspace: Annex UN GGE 2019/2021*, 2021; Germany, *Position Paper on the Application of International Law in Cyberspace*, 2021; New Zealand, *The Application of International Law to State Activity in Cyberspace*, 1 December 2020; Finland, *International Law and Cyberspace: Finland's National Position*, 2020; French Ministry of the Armed Forces, *Droit international appliqué aux opérations dans le cyberespace*, 2019. For the views of MSs of the Organization of American States, see Organization of American States, *Improving Transparency: International Law and State Cyber Operations (Fourth Report)*, OEA/Ser.Q, CJI/doc. 603/20 rev.1, 5 March 2020, pp. 18–20; Organization of American States, *Binding and Non-Binding Agreements: Final Report*, OEA/Ser.Q, CJI/doc. 615/20 rev.1, 7 August 2020, pp. 28–32. See, generally, Tallinn Manual 2.0, above note 21, Rules 1–4; Nicholas Tsagourias, "The Legal Status of Cyberspace: Sovereignty Redux?", in N. Tsagourias and R. Buchan (eds), above note 10. *Contra* Jeremy Wright, "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.

113 Permanent Court of Arbitration, *Island of Palmas*, 2 RIAA, 4 April 1928, p. 829.

114 See, for example, the cyber security statements listed in above note 112. See also Tallinn Manual 2.0, above note 21, Rule 1.

115 Contrast, for example, the position of Finland with that of France (see above note 112). See also Tallinn Manual 2.0, above note 21, Rule 4 and accompanying commentary. For a review of this State practice, see R. Buchan and I. Navarrete, above note 10.

116 For support for this approach, see R. Buchan, above note 10, Chap. 3; Kevin Jon Heller, "In Defense of Pure Sovereignty in Cyberspace", *International Law Studies*, Vol. 97, 2021.

117 See, for example, Glenn Sulmasy and John Yoo, "Counterintuitive: Intelligence Operations and International Law", *Michigan Journal of International Law*, Vol. 28, No. 3, 2006, p. 625.

118 Iñaki Navarrete and Russell Buchan, "Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions", *Cornell International Law Journal*, Vol. 51, No. 4, 2009, p. 897.

Having said that, we will now consider the 2018 OPCW and 2022 ICRC incidents and assess their legality under the principle of State sovereignty. As we recalled in the introduction to this article, the Netherlands alleged that Russia had attempted to hack the OPCW, which is an IO based in The Hague.[119] More specifically, the Netherlands claimed that Russian agents had parked a vehicle outside the OPCW's premises that was fitted with sophisticated surveillance equipment and which would enable them to hack into the computer networks and systems of the organization.[120] The Netherlands maintained that it had foiled the hack before it could commence[121] and proceeded to denounce the Russian actions as undermining the international rule of law without specifying which rules were implicated.[122]

In light of the preceding discussion, the hack would have breached a number of legal obligations owed to the OPCW by Russia as an MS. First, the hack would have breached the privileges and immunities contained in Article VIII of the Chemical Weapons Convention,[123] an agreement to which Russia is a party even though it has not signed a further agreement on privileges and immunities with the OPCW as other States Parties have.[124] The hack would have also breached the CIL on privileges and immunities, as discussed in the above subsection on "Privileges and Immunities under Customary International Law". Second, it would have breached the principle of GF as explained in the preceding section.

As far as the Netherlands as the host State is concerned, the principle of sovereignty comes to the fore. First, the fact that Russian agents had entered the Netherlands and operated within its territory and jurisdiction without its consent constitutes a breach of its sovereignty.[125] Second, the hack would have breached the Netherlands' sovereignty if the Russian agents had utilized Dutch cyber infrastructure to gain access to the OPCW's computer networks and systems. In this respect, it is important to recall the Netherlands' approach to sovereignty in cyberspace. According to the Netherlands, the principle of State sovereignty applies to cyberspace and "States have exclusive authority over the physical, human and immaterial (logical or software-related) aspects of cyberspace within their territory". The Netherlands further asserts that sovereignty is violated if

119 "How the Dutch Foiled Russian 'Cyber-Attack' on OPCW", *BBC News*, 4 October 2018, available at: www.bbc.co.uk/news/world-europe-45747472.

120 "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation", above note 5.

121 Remarks by the Minister of Defense, The Hague, 4 October 2018, available at: www.justice.gov/opa/page/file/1098576/download.

122 See "Netherlands Defence Intelligence and Security Service Disrupts Russian Cyber Operation", above note 5: "The Netherlands shares the concerns of other international partners regarding the damaging and undermining [nature of] the GRU's [Russian military intelligence] actions. It supports the conclusion, presented today by the UK, that GRU cyber operations such as this one undermine the international rule of law."

123 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, 1993, Art. VIII(E), available at: www.opcw.org/chemical-weapons-convention/articles/article-viii-organization.

124 For a list of these agreements, see: www.opcw.org/resources/opcw-agreements.

125 ICJ, *Nicaragua*, above note 50, para. 251.

there is "1) infringement upon the target State's territorial integrity; and 2) there has been an interference with or usurpation of inherently governmental functions of another state".[126] It seems that the Netherlands does not require physical damage or impose any threshold but defines a breach of sovereignty in qualitative terms – that is, according to the target of the interference. The OPCW hack would thus violate the first prong of the definition, provided that Dutch cyber infrastructure was used.

Regarding the 2022 ICRC hack, at the time of writing the identity of the perpetrator has not been established, but assuming that it was a State, the question arises as to whether the hack breaches Switzerland's sovereignty. The Swiss position is that "state sovereignty protects information and communication technologies (ICT) infrastructure on a state's territory against unauthorised intrusion or material damage" and that a breach of sovereignty can be established on two alternative bases: first, where the cyber operation violates its territorial integrity, and second, where the cyber operation interferes with or usurps an inherently governmental function. Again, these views are not expressed in categorical terms, and the Swiss statement goes on to mention

> i) incidents whereby the functionality of infrastructure or related equipment has been damaged or limited, ii) cases where data has been altered or deleted, interfering with the fulfilment of inherently governmental functions such as providing social services, conducting elections and referendums, or collecting taxes, and iii) situations in which a state has sought to influence, disrupt or delay democratic decision-making processes.[127]

It follows that the answer to the question of whether the ICRC hack breached Switzerland's sovereignty is not clear-cut. From the available information, the hack does not fall within the three scenarios mentioned above because it did not affect the functionality of Swiss infrastructure, delete or alter data, or influence decision-making – but again, these scenarios are not exhaustive. However, the hack may have breached the principle of State sovereignty provided that it involved unauthorized intrusion into Swiss cyber infrastructure.

To conclude this section, we contend that hacking operations against IOs breach the sovereignty of the host State or the sovereignty of any other State on whose cyber infrastructure the IO's targeted data or servers are located if the hacking involves unauthorized intrusion into the State's cyber infrastructure. We recognize that this describes the lowest threshold of violability and that the threshold can increase to the removal of functionality or damage, but this does not detract from the fact that hacking under certain circumstances can breach the sovereignty of the host State or the State which hosts the IO's servers and data.

126 The Netherlands, "Letter to the Parliament on the International Legal Order in Cyberspace: Appendix: International Law in Cyberspace", 5 July 2019, pp. 2–3, available at: www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.

127 Switzerland, above note 112, pp. 2–3.

Conclusion

IOs perform critically important functions and it is essential that they can maintain the confidentiality and integrity of their data. This article has examined which international legal rules can be called upon to protect IOs from hacking operations committed by States. It has demonstrated that hacking by MSs breaches the privileges and immunities granted to IOs by their constitutive treaties and other related treaties (such as specific agreements on privileges and immunities or headquarters agreements). These instruments usually provide for the inviolability of an IO's premises, property, assets, archives, documents and correspondence. Hacking by NMSs also breaches the privileges and immunities of IOs, which are established in CIL on the basis of a general practice accompanied by *opinio juris* and because they attach to the objective legal personality of IOs. Moreover, this article has argued that hacking operations by MSs and NMSs breach the principle of GF, which imposes certain obligations upon them in their relations with IOs. In particular, hacking impinges on the *pacta sunt servanda* rule, the duty to respect the legal personality of IOs, the postulates of loyalty, due regard and cooperation, and the obligation not to abuse rights. Finally, the principle of State sovereignty offers IOs indirect protection from hacking insofar as this activity breaches the sovereignty of the host State or any other State if its cyber infrastructure is penetrated in order to commit the hack.