International Review of the Red Cross (2025), **107** (928), 401–428.
The Military
doi:10.1017/S1816383125000190

IRRC

Inviolability in the digital era: The ICRC's Agreement on Privileges and Immunities with Luxembourg

Andrea Raab-Gray[1] and **Massimo Marelli**[2,3]
[1]Legal Counsel, International Committee of the Red Cross, Delegation for Cyberspace and Global Cyber Hub, Luxembourg
[2]Head of Data Protection Office, International Committee of the Red Cross, Geneva, Switzerland
[3]Fellow, European Centre on Privacy and Cybersecurity, Maastricht University, Maastricht, Netherlands
Corresponding author: Andrea Raab-Gray; Email: araab@icrc.org

The authors wish to specially thank Eve La Haye for her immense support, guidance and wisdom in drafting this piece. The authors also wish to thank Simon Brunschwig and Sankalp Ghatpande for their incredibly helpful feedback, both on legal and technical aspects.

The advice, opinions and statements contained in this article are those of the author/s and do not necessarily reflect the views of the ICRC. The ICRC does not necessarily represent or endorse the accuracy or reliability of any advice, opinion, statement or other information provided in this article.

Abstract

As the International Committee of the Red Cross (ICRC) and other international organizations (IOs) are undergoing significant digital transformation and operate in an increasingly digitalized environment, questions as to how they can continue to ensure their information security are becoming more acute. Legal tools to protect IOs from harm in the digital age are central in this regard, alongside technical and organizational measures. This article focuses on one specific legal tool that can be used to foster IOs' information security, namely legal interpretations of the concept of inviolability. Specifically, the article explores how the Agreement on the ICRC's privileges and immunities in Luxembourg interprets the scope of the concept of inviolability, and the obligations arising under it.

Keywords: privileges and immunities, international organizations, information security, inviolability, digital transformation, positive obligations, Delegation for Cyberspace, status agreement, ICRC, cyber

Often driven by the ambition to increase their operational efficiency and effectiveness,[1] the International Committee of the Red Cross (ICRC) and a number of other international organizations (IOs) have been undergoing significant digital transformation, which some hope to further accelerate.[2] Yet, reaping the benefits of digital transformation typically requires relying on complex cyber infrastructure.[3] This comprises the communications, storage and computing devices on which information systems are built and operate,[4] including network connections, cabling and physical servers, as well as software. Cyber infrastructure may involve proprietary or leased components, and might be set up in a data centre that belongs to or is entirely controlled by the IO, or a data centre which belongs to a third party. Moreover, the use of digital services often requires that third parties, such as service providers, process data on behalf of the IO.[5] As such, digital transformation may entail that

1 For further detail, see United Nations (UN) Office for the Coordination of Humanitarian Affairs, "From Digital Promise to Frontline Practice: New and Emerging Technologies in Humanitarian Action", 19 April 2021, available at: www.unocha.org/publications/report/world/digital-promise-frontline-practice-new-and-emerging-technologies-humanitarian-action (all internet references were accessed in April 2025).

2 See e.g. ICRC, *Institutional Strategy 2024–2027*, November 2023, pp. 24 ff., available at: www.icrc.org/sites/default/files/wysiwyg/Activities/icrc_institutional_strategy_2024-2027.pdf; UN, "UN Launches Strategy for Digital Transformation of Peacekeeping", press release, 18 August 2021, available at: https://news.un.org/en/story/2021/08/1098072; International Criminal Court (ICC), *Office of the Prosecutor Strategic Plan 2023–2025*, Strategic Goal 3, "Make the Office a Global Technology Leader", p. 14, available at: www.icc-cpi.int/sites/default/files/2023-08/2023-strategic-plan-otp-v.3.pdf.

3 This article uses the terms "digital" and "cyber" synonymously.

4 See Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, Cambridge, 2017 (Tallinn Manual), p. 564.

5 For the purposes of this article, the term "process" includes any operation or set of operations which is performed on data, including hosting, computing, backing up and sub-processing.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

data is processed on, and transferred to and from, a range of technical equipment. This equipment may be located in manifold different States, and IOs might exercise varying degrees of physical control over it.

In addition to their own digital transformation, the ICRC and IOs more generally find themselves in an increasingly digitalized operating environment, which poses growing challenges to IOs' information security. Indeed, the United Nations (UN) International Computing Centre reported a 170% increase in "malicious activities of interest" against its partner organizations, chiefly UN agencies, in 2023, as compared to 2022.[6]

The digital era thus presents IOs with a pivotal challenge: how can IOs maintain their information security, understood as protection against unauthorized access, use, disclosure, modification, destruction or disruption of cyber infrastructure and information, including data,[7] in light of this set-up? Put differently, how can the many geographically separate locations and technical devices processing an IO's data – and of course the data itself – be effectively protected from outside interference?[8]

It is in this context that, alongside technical and organizational measures, IOs have been considering how privileges and immunities can contribute to their information security. There exists State practice and scholarship on how diplomatic privileges and immunities are to be interpreted to apply in relation to data and cyber infrastructure. However, the common practice of IOs and their host States in protecting IOs' data, cyber infrastructure and data centres remains to be further unpacked.

This is what the present article sets out to do, drawing on the experience of the ICRC. Prior to establishing its Delegation for Cyberspace in 2022, which is based in Luxembourg and has since evolved into the ICRC's Global Cyber Hub, the ICRC and Luxembourg concluded the Agreement on the Status and Privileges and Immunities of the International Committee of the Red Cross between the Grand Duchy of Luxembourg and the International Committee of the Red Cross (the Agreement).[9] Signed on 1 June 2022 and entered into force on 5 September 2023, the Agreement provides the ICRC with the privileges and immunities that it is usually granted by States, such as immunity from legal process, inviolability of archives and

6 See UN International Computing Centre, *Cyber Threat Landscape Report 2023*, May 2024, p. 5, available at: www.unicc.org/wp-content/uploads/2024/07/2023-Cyber-Threat-Landscape-Report-1.pdf.

7 See the definition in the National Institute of Standards and Technology glossary, available at: https://csrc.nist.gov/glossary/term/information_security.

8 For a detailed discussion of the challenges facing IOs, see Massimo Marelli, "Hacking Humanitarians: Defining the Cyber Perimeter and Developing a Cyber Security Strategy for International Humanitarian Organizations in Digital Transformation", *International Review of the Red Cross*, Vol. 102, No. 913, 2020.

9 Agreement on the Status and Privileges and Immunities of the International Committee of the Red Cross between the Grand Duchy of Luxembourg and the International Committee of the Red Cross, 1 June 2022 (entered into force 5 September 2023), available at: www.stradalex.lu/fr/slu_src_publ_leg_mema/toc/leg_lu_mema_202309_587/doc/mema_etat-leg-loi-2023-09-05-a587-jo. For further information on the ICRC's Delegation for Cyberspace and Global Cyber Hub, see Massimo Marelli, "Opening an ICRC Delegation for Cyberspace", *EJIL: Talk!*, 9 February 2023, available at: www.ejiltalk.org/opening-an-icrc-delegation-for-cyberspace/.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

personal functional immunity for ICRC staff – but in addition to those, it also contains specific provisions to protect the ICRC's data and cyber infrastructure, as well as any data centres used by the ICRC, from interference, including by cyber means. In doing so, the Agreement fleshes out how inviolability should be interpreted to provide the ICRC with the tools to do its job in the digital age.

This article analyzes the host State obligations set out in the Agreement stemming from the concept of inviolability, and discusses how some novel provisions in the Agreement constitute an interpretation of the concept of inviolability in an increasingly digital environment. It develops this analysis in the context of broader practice of IOs and States, as well as academic commentary. The scope of the article is limited to the concept of inviolability, given that, as will be shown below, this is the most relevant legal construct related to IOs' privileges and immunities for protecting data, cyber infrastructure and data centres from interference. The article will refrain, however, from considering whether inviolability of IOs' archives, property and assets, and/or premises, or any obligations flowing from such inviolability, have become customary international law, and neither will it discuss other concepts or norms of international law which might also serve to protect an IO's data, data centres and cyber infrastructure from interference, such as good faith[10] or rules of international humanitarian law (IHL).[11]

The article proceeds in three parts. The first part sets the scene by outlining the ICRC's mandate, working modalities and legal status, explaining the importance of information security for the ICRC, and discussing how inviolability can foster information security. The second part analyzes the scope of inviolability under the Agreement between the ICRC and Luxembourg, discussing how data, data centres and cyber infrastructure can fall within the notions of premises, archives, and property and assets, to which inviolability typically applies. The third part dissects cyber-related obligations under the Agreement linked with concept of inviolability.

Setting the scene: The ICRC, its legal status, and the importance of information security

The ICRC and its legal status

The ICRC is a neutral, independent and impartial organization which States have vested with the exclusively humanitarian mandate to assist and protect persons affected by armed conflict and other situations of violence. The ICRC also endeavours to prevent suffering by promoting and strengthening IHL. In carrying

10 On this, see Russell Buchan and Nicholas Tsagourias, "Hacking International Organizations: The Role of Privileges, Immunities, Good Faith and the Principle of State Sovereignty", *International Review of the Red Cross*, Vol. 104, No. 919, 2022, pp. 1186–1194.

11 On this, see Laurent Gisel, Tilman Rodenhäuser and Knut Dörmann, "Twenty Years On: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts", *International Review of the Red Cross*, Vol. 102, No. 913, 2020, p. 329.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

out this mandate, the ICRC strictly observes the Fundamental Principles of the Red Cross and Red Crescent Movement (the Movement), including neutrality, independence and impartiality, as well as the "do no harm" principle and its standard working modalities, including confidentiality.

"Do no harm" means ensuring that the ICRC's action does not harm the persons whom it seeks to serve. The ICRC's confidential approach entails that the ICRC engages with States and parties to armed conflict through bilateral confidential dialogue, in which it raises humanitarian concerns and allegations of violations of IHL. The ICRC does not, as a rule, share the contents of this dialogue with any third parties. Importantly, the ICRC's confidential approach is a means to an end, not an end in itself. It is not tantamount to silence in the face of mistreatment or other breaches of international law; rather, the ICRC's experience has shown that maintaining confidentiality enables it to avoid politicization. This, in turn, fosters openness, candidness and willingness to allow the ICRC to assist affected persons, particularly in fragile settings such as prisons. The ICRC's confidential approach is the reason why oftentimes, it is the sole organization whose presence is accepted in certain contexts – the only organization with "boots on the ground", able to administer humanitarian aid. States, other actors and individuals benefiting from the ICRC's action expect the ICRC to adhere to its confidentiality.[12]

Turning to its legal status, the ICRC was founded in 1863 as a private association under Swiss law, at a time when "international organizations" did not exist as an international legal construct. In addition to the fact that it was not founded by virtue of a treaty between two or more States, the ICRC's set-up differs from that of intergovernmental organizations as subsequently conceived of and established: it does not have a governing body comprised of States, but its Assembly is made up of individuals of Swiss citizenship. Nevertheless, the ICRC's legal status has evolved over time, such that it has come to be regarded as having an international legal personality *sui generis*, equivalent to that of international intergovernmental organizations. The following factors attest to this.[13]

First, the ICRC received its mandate from States in international treaties and other international legal instruments, including the 1949 Geneva Conventions, their 1977 Additional Protocols, and resolutions of the International Conference of the Red Cross and Red Crescent.[14] Thus, "while the ICRC's existence and governance

12 See also Elem Khairullin, "5 Things that Make ICRC Confidential Information Unsuitable for Legal Proceedings", *Humanitarian Law and Policy Blog*, 31 January 2019, available at: https://blogs.icrc.org/law-and-policy/2019/01/31/5-things-make-icrc-confidential-information-unsuitable-legal-proceedings/.

13 For a more detailed analysis of the evolution of the ICRC's status, 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, 2016, pp. 320–329.

14 Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949, 75 UNTS 31 (entered into force 21 October 1950) (GC I); Geneva Convention (II) for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 12 August 1949, 75 UNTS 85 (entered into force 21 October 1950) (GC II); Geneva Convention (III) relative to the Treatment of Prisoners of War of 12 August 1949, 75 UNTS 135 (entered into force 21 October 1950) (GC III); Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War of 12 August 1949, 75 UNTS 287 (entered into force 21 October 1950) (GC IV); Protocol

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

are not mandated by States, its functions and activities are", in a manner similar to international intergovernmental organizations.[15] Importantly, at no point have States suggested that the ICRC's governance should change. On the contrary, the fact that the ICRC's governing body is made up of Swiss nationals has been perceived as ensuring the organization's neutrality.[16]

Second, by virtue of bilateral international agreements and national legislation, the ICRC enjoys privileges and immunities in more than 110 States around the globe at the time of writing. These privileges and immunities largely correspond to, and are indeed modelled on, those accorded to the UN under the 1946 Convention on the Privileges and Immunities of the United Nations (General Convention).[17] As they are generally only bestowed upon IOs, the fact that the ICRC is granted privileges and immunities demonstrates that States are regarding the ICRC as an IO. Indeed, many States included a clause in agreements or national legislation granting privileges and immunities to the ICRC, in which they expressly acknowledge the ICRC's legal status as equivalent to that of an international intergovernmental organization.

Third, in practice, the ICRC enjoys diplomatic treatment: ministries of foreign affairs are the ICRC's main interlocutor, the organization is often granted the right to use diplomatic plates for its vehicles, and ICRC heads of delegation are generally treated in a manner equivalent to heads of diplomatic missions or IOs' country representatives.

Finally, the ICRC has been granted observer status at the UN and other international or regional organizations – a status usually reserved for international intergovernmental organizations.[18]

Additional (I) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts, 1125 UNTS 3, 8 June 1977 (entered into force 7 December 1978) (AP I); Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 1125 UNTS 609, 8 June 1977 (entered into force 7 December 1978) (AP II). The following provisions of the Geneva Conventions make specific reference to the ICRC: GC I, Arts 3, 9, 10, 11, 23; GC II, Arts 3, 9, 10, 11; GC III, Arts 3, 9, 10, 11, 56, 72, 73, 75, 79, 81, 123, 125, 126; GC IV, Arts 3, 10, 11, 12, 14, 30, 59, 61, 76, 96, 102, 104, 108, 109, 111, 140, 142, 143. In accordance with Article 10 of GC I–III and Article 11 of GC IV, the ICRC can – and in practice does – exercise many of the functions entrusted to the Protecting Power by the following provisions: GC I, Arts 8, 16, 23, 48; GC II, Arts 8, 19, 44, 49; GC III, Arts 20, 121, 122, 128; GC IV, Arts 9, 23, 24, 35, 39, 42, 43, 45, 49, 52, 55, 60, 71, 72, 74, 75, 83, 98, 101, 105, 113, 129, 131, 137, 145. The relevant provisions in AP I are Articles 5, 6, 33, 78, 81, 97 and 98. Articles 2, 11, 45, 60, 70 and 84 of AP I deal with the Protecting Power. The status of the ICRC is also recognized in Article 24 of AP II. The role and functions of the ICRC are helpfully summarized in Article 5 of the Statutes of the International Red Cross and Red Crescent Movement, adopted by the 25th International Conference of the Red Cross at Geneva in 1986 and amended in 1995 and 2006 (entered into force 8 November 1986).

15 E. Debuf, above note 13, p. 324.

16 *Ibid.*, p. 323.

17 Convention on the Privileges and Immunities of the United Nations, 1 UNTS 15 and 90 UNTS 327, 13 February 1946 (entered into force 17 September 1946) (General Convention). See also Convention on the Privileges and Immunities of the Specialized Agencies, 33 UNTS 261, 21 November 1947 (entered into force 2 December 1948) (Convention on Specialized Agencies).

18 See e.g. UNGA Res. 45/6, "Observer Status for the International Committee of the Red Cross, in Consideration of the Special Role and Mandates Conferred upon It by the Geneva Conventions of 12 August 1949", 16 October 1990.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

The foregoing demonstrates that the ICRC's legal status has evolved over time to be equivalent to that of international intergovernmental organizations.

The importance of information security for the ICRC's ability to carry out neutral, independent and impartial humanitarian action and observe its working modalities

Ensuring its information security is key for the ICRC to be able to carry out neutral, independent and impartial humanitarian action in line with its working modalities in the digital era – and to be seen to be doing so.

In the first place, information security is essential for the ICRC's ability to adhere to the principle of "do no harm". The ICRC operates in volatile environments, such as armed conflicts and other situations of violence, and as such, it often generates, collects and/or processes highly sensitive data. Unauthorized disclosure of, access to or extraction of such data by States or other actors can further compound the harms facing communities who are often already caught in crossfire: for instance, the disclosure of affected persons' medical data without their consent can curtail their agency and exacerbate their vulnerability to additional harms. In particular, the unauthorized public disclosure of medical data of survivors of sexual violence can lead to their ostracization and that of any children born out of rape. Thus, persons whom the ICRC seeks to serve might reject the ICRC's assistance if they fear that their data might be accessed by third parties and potentially used for purposes other than those initially intended.

Relatedly, protecting the ICRC's data, data centres and cyber infrastructure from unauthorized access is key to maintaining the trust of its stakeholders, particularly in light of the organization's confidential approach in engaging with States and other actors. These stakeholders all expect the ICRC to take measures necessary to maintain its confidentiality, so unauthorized interference with data pertaining to this dialogue, or the infrastructure on which it is processed, might cause States, affected persons and other actors to lose their trust in the ICRC and in its neutrality.[19] With confidentiality often being the premise for acceptance of the ICRC's presence in a given context, unauthorized access to and disclosure of data pertaining to the organization's confidential bilateral dialogue might also jeopardize the safety of ICRC staff, who often risk their lives to help others. In light of this, the ICRC's information, including data, and the institution's confidentiality are protected not only by specific privileges and immunities but also by virtue of a privilege of non-disclosure unique to the ICRC.[20]

19 See also Massimo Marelli, "The Law and Practice of International Organizations' Interactions with Personal Data Protection Domestic Regulation: At the Crossroads between the International and Domestic Legal Orders", *Computer Law Security Review*, Vol. 50, 2023, p. 5.

20 International Criminal Tribunal for the former Yugoslavia, *Prosecutor v. Simić et al.*, Case No. IT-95-9, Decision on the Prosecution Motion under Rule 73 for a Ruling Concerning the Testimony of a Witness, 27 July 1999, paras 72–74. For further information on the ICRC's confidential approach, see ICRC, "Memorandum: The ICRC's Privilege of Non-Disclosure of Confidential Information", *International Review of the Red Cross*, Vol. 97, No. 897–898, 2016.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

The above illustrates that information security is and has always been a prerequisite for the ICRC to maintain its ability to serve affected communities. Yet, in the digital age and in light of its stated ambition to accelerate digital transformation,[21] the ICRC requires certain legal tools to carry out – and to be seen to be carrying out – its mandate while adhering to the above working modalities. These tools include adequate interpretations of the scope of, and obligations flowing from, inviolability.

The link between inviolability and information security

Thus far, this section has focused on the ICRC. At this juncture, it is helpful to take a step back and consider *why* the concept of inviolability is important in relation to the information security of IOs more generally.

While the privileges and immunities of States and their representatives are based on State equality,[22] the primary raison d'être for IOs' privileges and immunities is the principle of functionality. This means that privileges and immunities seek to ensure that IOs can fulfil the mandates entrusted to them by the international community independently, and as efficiently and effectively as possible.[23]

Often modelled on equivalent provisions in the 1961 Vienna Convention on Diplomatic Relations (VCDR),[24] instruments containing privileges and immunities for IOs typically provide for inviolability of an IO's premises,[25] as well as its archives and in general all documents, in whatever form, belonging to the IO or held by it, wherever located.[26] They also usually enshrine inviolability of property and assets by referring to the immunity of an IO's property and assets, wherever located and by whomsoever held, from search, requisition, confiscation, expropriation or any other form of interference, whether by executive, administrative, judicial or legislative action.[27] Though these provisions typically employ the term

21 ICRC, above note 2, pp. 24 ff.

22 See e.g. International Court of Justice (ICJ), *Jurisdictional Immunities of the State (Germany v. Italy: Greece Intervening)*, Judgment, 3 February 2012, para. 57.

23 Compare Charter of the United Nations, 1 UNTS XVI, 26 June 1945 (entered into force 24 October 1945), Art. 105; E. Debuf, above note 13, p. 333.

24 Vienna Convention on Diplomatic Relations, 500 UNTS 95, 18 April 1961 (entered into force 24 April 1964) (VCDR). See Lance Bartholomeusz, "Inviolability of Premises (Article II Section 3 General Convention)", in August Reinisch (ed.), *The Conventions on the Privileges and Immunities of the United Nations and Its Specialized Agencies: A Commentary*, Oxford University Press, Oxford, 2016, para. 1; Gian Luca Burci, "Inviolability of Archives (Article II Section 4 General Convention)", in A. Reinisch (ed.), *ibid.*, para. 1.

25 General Convention, above note 17, Art. II, Section 3; 1947 Convention on Specialized Agencies, above note 17, Art. III, Section 5; Agreement on the Privileges and Immunities of the International Criminal Court, 2271 UNTS 3, 9 September 2002 (entered into force 22 July 2004) (APIC), Art. 4; Agreement between the Republic of Austria and the Organization for Security and Co-Operation in Europe (OSCE) Regarding the Headquarters of the Organization for Security and Co-operation in Europe, 14 June 2017 (Agreement between Austria and the OSCE), Art. V, Section 7.

26 General Convention, above note 17, Art. II, Section 4; Convention on Specialized Agencies, above note 17, Art. III, Section 6; Agreement between Austria and the OSCE, above note 25, Art. V, Section 8. See also APIC, above note 25, Art. 7.

27 See e.g. General Convention, above note 17, Art. II, Section 3; APIC, above note 25, Art. 6(2).

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

"immunity", conceptually this is better understood as an "inviolability" in light of the following considerations.[28] Many, if not all, instruments granting privileges and immunities to IOs distinguish between immunity and inviolability as distinct concepts. Whilst both prohibit interference with an IO's independence, there are two cardinal differences: first, inviolability does not presuppose any link with legal proceedings, whilst immunity is only triggered whenever there is a nexus to legal proceedings,[29] and second, inviolability entails not only a negative obligation to refrain from interference but also a positive obligation to protect the object of inviolability.[30]

From a legal perspective, inviolability is crucial in the digital era for an IO's information security, as there currently exists no treaty outside the realm of IOs' privileges and immunities which contains a norm specifically prohibiting interference with an IO's data, data centres or cyber infrastructure.[31] In contrast, where a State has undertaken a legal obligation to respect the inviolability of an IO's data, data centre and cyber infrastructure, interference with those objects might cause that State to be in breach of the obligations that it owes to the IO. These considerations are without prejudice to any possible norm of customary international law, which falls outside the scope of this article.

From a practical viewpoint, whilst States can opt to process data on their own territory and have the authority to protect the corresponding facilities, IOs lack such authority and territory of their own. They are therefore, to a certain extent, dependent on the host State to refrain from interference and provide a certain degree of protection, without jeopardizing the IO's independence.

In light of the above, inviolability, if interpreted adequately, can constitute an essential legal safeguard for data, cyber infrastructure and data centres of an IO against outside interference. This is why clarifying the scope and cyber-related positive and negative obligations stemming from inviolability is a central question in relation to IOs' information security. The following sections discuss how the Agreement between Luxembourg and the ICRC interprets inviolability.

28 See also Tom Ruys, "Immunity, Inviolability and Countermeasures – a Closer Look at Non-UN Targeted Sanctions", in Tom Ruys and Nicolas Angelet (eds), *Cambridge Handbook on Immunities and International Law*, Cambridge University Press, Cambridge, 2019, p. 691.

29 *Ibid.*, p. 690.

30 See e.g. *ibid.*, above note 28, p. 690. With a view to positive obligations relating to archives, in light of the fact that IOs' inviolability of archives stems from the equivalent protection of the archives of diplomatic missions, see Eileen Denza, *Diplomatic Law: Commentary on the Vienna Convention on Diplomatic Relations*, 4th ed., Oxford University Press, Oxford, 2016, p. 158: "In the first place, the expression 'inviolable' was deliberately chosen by the International Law Commission (ILC) to convey both that the receiving State must abstain from any interference through its own authorities and that it owes a duty of protection of the archives in respect of unauthorized interference by others".

31 See "Scenario 04: A State's Failure to Assist an International Organization", *Cyber Law Toolkit*, para. L3, available at: https://cyberlaw.ccdcoe.org/wiki/Scenario_04:_A_State%E2%80%99s_failure_to_assist_an_international_organization. On IHL, see L. Gisel, T. Rodenhäuser and K. Dörmann, above note 11.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

The scope of inviolability: Conceptualizing data, cyber infrastructure and data centres within the notions of "premises", "archives", and "property and assets"

This section analyzes how the Agreement between the ICRC and Luxembourg defines the scope of inviolability. As noted above, many instruments provide for the inviolability of "archives", "property and assets", and "premises". Thus, after explaining the terminology of the Agreement, this section examines the extent to which the Agreement places data, data centres and cyber infrastructure within the ambit of the notions of "archives", "property and assets", and "premises".

Terminology of the agreement

The Agreement distinguishes between "Data Centres" used by the ICRC, "Data and Information Systems", and "Equipment and Licenses". In the remaining parts of this article, terms will be capitalized whenever reference is made to the terminology of the Agreement.

Article 1(a) defines a Data Centre benefiting from the protections of the Agreement as "the part of a facility located in Luxembourg and provided through a lease agreement by Luxembourg or directly rented from a local service provider, and used to host Data and Information Systems, as well as the Equipment and Licences". Thereby, the Agreement encompasses both government-provided data centres and commercial data centres which are geographically distinct from the ICRC's offices in Luxembourg.

Under Article 1(b), "Data and Information Systems" means "assets that are stored and processed on the Equipment and associated components, such as telecommunications and storage systems. It includes software and solutions installed on the Equipment as well as the data processed and stored therein."

Article 1(c) stipulates that the term "Equipment and Licenses" refers to

> the assets used for the storing and processing of Data and Information Systems and associated components, such as telecommunications and storage systems. This includes assets such as computers and servers and racks, virtual machines, network devices like routers and switches, cabling and patching and power distribution unit[s], and Virtual Private Networks.

The definitions of "Data and Information Systems" and "Equipment and Licenses" are both modelled on the agreement between Luxembourg and Estonia concerning Estonia's data embassy.[32]

Pursuant to Article 1(d), the ICRC's Data Centres, as well as the Data and Information Systems and Equipment and Licenses which the ICRC holds in a Data Centre or at its physical delegation, together constitute the "ICRC Cyber

32 See Agreement between the Republic of Estonia and the Grand Duchy of Luxembourg on the Hosting of Data and Information Systems, 20 June 2017, Art. 1(c)–(d), available at: www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

Infrastructure". This definition was chosen for ease of drafting, to avoid convoluted formulations within the Agreement. It encompasses all Data Centres, Equipment and Licenses, and Data and Information Systems which the ICRC uses, irrespective of whether they are located at the ICRC's delegation, the government-provided Data Centre or a commercial Data Centre. To ensure internal consistency, and in deviation from the terminology of the Agreement, this article uses the term "cyber infrastructure" when referring to both Data and Information Systems and Equipment and Licenses. Data Centres will be referred to separately.

The term "data" is not specifically defined in the Agreement, though it is used within the ambit of the term "Data and Information System", but also separate and independent of that term. Applying the customary interpretation rule reflected in Article 31 of the 1969 Vienna Convention on the Law of Treaties,[33] the terms of the Agreement are to be interpreted given their ordinary meaning, in good faith and taking into account the treaty's object and purpose. The Cambridge Dictionary defines the term "data" *inter alia* as "information in an electronic form that can be stored and used by a computer".[34] Echoing the principle of functionality, the preamble of the Agreement specifies that the object and purpose of the Agreement is to grant the ICRC "adequate privileges and immunities under international and national law to operate its Delegation for Cyberspace based in Luxembourg in full conformity with its fundamental principles of humanity, neutrality, impartiality and independence and its standard working modalities, in particular confidentiality". The broad ordinary meaning of the term "data" and the fact that the Agreement seeks to enable the ICRC to operate the Delegation in keeping with its working modalities and the Fundamental Principles militate in favour of a wide interpretation of the term "data" in the context of the Agreement. As such, for the purposes of the Agreement, "data" must be understood to cover both content data and metadata – i.e., "data about data", such as data regarding access to certain files, user information etc.

In sum, the scope of the Agreement encompasses all data, as well as cyber infrastructure and Data Centres in Luxembourg. The logical next step is to discuss how the Agreement interprets the terms "archives", "property and assets" and "premises", and how it fits the aforementioned terminology within these notions.

Data and cyber infrastructure as archives

Article 6(1) of the Agreement provides that "all documents and data (including electronic documents), as well as all Data and Information Systems, and all Equipment and Licenses, which belong to, [or] are used or held by the ICRC" constitute archives, and are thus "inviolable wherever located". This includes "data held in or otherwise processed through servers, server rooms, and any other device containing data hosted by the ICRC". Several elements of this provision require discussion.

33 See ICJ, *Case Concerning the Territorial Dispute (Libyan Arab Jamahiriya v. Chad)*, Judgment, 3 February 1995, para. 41.

34 "Data", *Cambridge Dictionary*, available at: https://dictionary.cambridge.org/dictionary/english/data#google_vignette.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

First, the fact that not only the content of the archives, e.g. data, is protected, but also the physical objects on which data is processed (that is, physical components of Data and Information Systems and all Equipment and Licenses), is in line with UN and State practice.[35]

Second, by referring to data "which belong to, are used or held" by the ICRC, the Agreement encompasses data, including metadata and content data in line with the analysis in the previous section, which is generated by the ICRC, as well as data which it collects or receives from others. In practice, this includes, for instance, personal data of staff, or information provided by persons benefiting from the ICRC's action. This delineation of the scope of inviolability is in keeping with the prevailing interpretation of the term "archives", which has been understood to include not only information that the IO itself has produced, but also information that it has collected or otherwise received.[36]

Third, in protecting data and cyber infrastructure as archives "wherever located" as well as data "belonging to or used by" the ICRC, even if such data is "held" by third parties, Article 6 of the Agreement protects not only data which the ICRC itself holds, but also that which is held or processed by third parties. This wide interpretation of the scope of inviolability aligns with broader IO and State practice on the notion of "wherever located": in the context of the UN, the phrase "wherever located" has been interpreted to mean that "[t]he protection enjoyed by the 'archives' of the UN, and the corresponding legal control that the UN Secretary-General can exercise over them, is not limited to documents, records, and information physically located or stored on UN premises".[37] In light of this, the UN seems to understand "archives" to include data and cyber infrastructure held by third parties, such as service providers, for instance for purposes of processing data in rendering digital services, including cloud-based services. This conforms with the practice of States and IOs, similarly suggesting that data indeed maintains its protection when processed in a cloud environment.[38] Cloud processing typically involves not only a main service provider on whose servers data is processed, but also third-party subprocessors who may have access to data in a public cloud environment. Thus, by recognizing that data processed in a cloud environment is covered by privileges and

35 See G. L. Burci, above note 24, paras 8, 10. See also *Cybersecurity in the United Nations System Organizations: Report of the Joint Inspection Unit*, UN Doc. JIU/REP/2021/3, 2021, para. 5; Tallinn Manual, above note 4, p. 220.

36 See G. L. Burci, above note 24, paras 15–18. See also Tallinn Manual, above note 4, p. 220.

37 G. L. Burci, above note 24, para. 49. See also Lord Mance in UK Supreme Court (UKSC), *R (on the Application of Bancoult No. 3) v. Secretary of State for Foreign and Commonwealth Affairs*, [2018] UKSC 3, 8 February 2018, para. 20.

38 European Data Protection Supervisor, *Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies*, 16 March 2018, para. 63. See also E. Denza, above note 30, pp. 162–163; Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation, *Implementation of the Virtual Data Embassy Solution: Summary Report of the Research Project on Public Cloud Usage for Government*, p. 14. Note that the Tallinn Manual, above note 4, p. 221, only refers to data in a private cloud environment and leaves the protection of data in a public cloud infrastructure unaddressed.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

immunities, State and IO practice suggests that data held by third parties continues to enjoy inviolability, thus assigning a wide meaning to the notion of "wherever located".

Case law and academic commentary further support this interpretation. Referring to Lord Sumption's judgment in the UK Supreme Court's *Bancoult (No. 3)* case, Buchan and Tsagourias assert that "where an IO passes data to or shares data with another actor and, in doing so, relinquishes control over it, those data can no longer be described as 'belonging to' or 'held by' the IO".[39] They propose a wide definition of the term "control", however, whereby an IO exercises control over data where it is able to "access, modify and delete the data or transfer it to another actor".[40] With this, Buchan and Tsagourias seem to refrain from requiring that the IO have *exclusive* control over the data – that is, the IO does not need to be the *only* entity to control the data. If this is so, following Buchan and Tsagourias, data processed by third parties, including in a public cloud environment, remains protected by inviolability so long as the IO is able to "access, modify and delete the data or transfer it to another actor".

In discussing the Court of Appeals decision in *Bancoult*, Denza considers that Article 24 of the VCDR bestowing inviolability on a diplomatic mission's archives "wherever they may be"

> must be construed to include cyberspace as well as computer storage facilities outside the receiving State if the protection of confidentiality required by Article 24 is to be effective under modern methods of recording and transmitting information. It seems clear that this is required in order to give proper effect to Article 24 as was intended by the original Parties.[41]

Similarly, in the *Tehran Hostages* case, the International Court of Justice (ICJ) found Iran to be in continued breach of Article 24 of the VCDR in light of "repeated statements by the militants occupying the Embassy, who claim to be in possession of documents from the archives, and by various government authorities, purporting to specify the contents thereof".[42] The ICJ would not have been able to find Iran in *continued* breach of Article 24 of the VCDR if the requirement of "control" was to be construed in a manner whereby the respective documents must be under the *exclusive* control of the diplomatic mission (or IO). In light of the above, Article 6 of the Agreement between the ICRC and Luxembourg reflects the legal views prevailing amongst States, IOs, case law and academia, whereby data remains part of an IO's archives even where it is processed by a third party, so long as the IO maintains

39 R. Buchan and N. Tsagourias, above note 10, p. 1179; UKSC, *Bancoult (No. 3)*, above note 37, para. 68.

40 R. Buchan and N. Tsagourias, above note 10, p. 1178: "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".

41 E. Denza, above note 30, pp. 166–167.

42 ICJ, *United States Diplomatic and Consular Staff in Tehran* (*United States of America v. Iran*), Judgment, 24 May 1980, para. 77.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

some control over that data. However, data need not be under the exclusive control of the IO.

For purposes of comprehensiveness, the raison d'être of inviolability ought to be addressed. Inviolability of archives serves to safeguard the confidentiality of an IO's data.[43] Providing data to service providers for purposes of processing or using cloud facilities does not in any way suggest that an IO intends to relinquish the confidentiality of that data. Indeed, in practice, contracts with service providers tend to contain confidentiality clauses requiring the service provider not to share data with any third parties, or make data public, without the consent of the IO.

In short, Article 6 of the Agreement delineates the scope of "archives" in a broad manner, encompassing data generated by or provided to the ICRC, as well as cyber infrastructure over which the ICRC has "control", in the sense that it can alter, grant access to or otherwise dispose of data. This includes data held by third parties for purposes of processing, which is in line with IO and State practice as well as case law and academic commentary.

Data centres as premises of an IO?

Article 5*bis* of the Agreement provides for inviolability of the portion of the Data Centre used by the ICRC, including both commercial and government-owned data centres. The Agreement is silent as to whether the Data Centre as defined above constitutes "premises" of the ICRC, and premises are regulated separately from the Data Centre, namely in Article 4 of the Agreement providing for the inviolability of the ICRC's premises. Beyond the Agreement, too, there seems to be no legal clarity either as to whether data centres can constitute an IO's premises.

With a view to IO practice, and in parallel to Article 1(i) of the VCDR, the term "premises" has been considered to comprise buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission.[44] For example, the premises of the UN thus encompass not only buildings owned by the UN but also those rented by it, as well as rented portions of buildings owned by others.[45] In light of this, and given that none of the above suggests that there is a limit to the number of buildings that can be used "for the purposes of the mission", it would appear arguable that segregated and specifically identified portions of data centres rented for purposes of an IO could constitute "premises". Importantly, however, the fact that the data of an IO is merely processed in a data centre, as would be the case for commercial cloud facilities, does not seem to suffice to consider the data centre or parts thereof "premises" of the IO.[46] This could be argued to translate into practice as follows: where an IO rents or is provided dedicated servers in a data

43 See G. L. Burci, above note 24, paras 1, 2. See also UKSC, *Bancoult (No. 3)*, above note 37, paras 20, 75; Tallinn Manual, above note 4, p. 221; E. Denza, above note 30, p. 161.

44 See L. Bartholomeusz, above note 24, para. 8. Some agreements define the perimeter of the premises specifically; see, for instance, Agreement between Austria and the OSCE, above note 25, Art. IV, Section 4.

45 L. Bartholomeusz, above note 24, para. 8.

46 See, in this sense, R. Buchan and N. Tsagourias, above note 10, p. 1176.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

centre owned by a third party, this could render these specific portions of the data centre "premises" of the IO. In contrast, where the IO does not rent or use dedicated servers, but its data is merely processed on servers of a third party along with the data of other customers, this does not make the data centre or portions thereof used to process the data "premises". It is worth pointing out, however, that data processed in either of those two scenarios in principle remains the IO's "archives" and as such is inviolable.

Nevertheless, there has been no explicit endorsement of the notion that data centres could constitute an IO's premises. At the same time, there are currently no indications precluding *per se* that data centres not exclusively used by an IO could constitute an IO's premises. As mentioned above, the Agreement is silent on this matter and does not expressly bring Data Centres geographically distinct from the ICRC's offices within the scope of the term "premises". It thus remains to be seen whether and how IOs' and States' legal views on this point will crystallize. Yet, even if they are not categorized as "premises" of the ICRC, Data Centres are specifically protected by the Agreement, as will be discussed further below.

Data and cyber infrastructure as property and assets?

Closely reflecting the wording of Article II(2) of the General Convention, Article 4(2) of the Agreement provides that the ICRC's property and assets are inviolable.[47] The Agreement takes the following approach toward conceptualizing data, Data and Information Systems and Equipment and Licenses as "property and assets".

Pursuant to Article 5*quater*, Equipment and Licenses which are "required to operate the Data Centre used by the ICRC and put in place on the premises of the Data Centre" constitute assets of the ICRC and shall enjoy immunity from every form of legal process. As immunity applies to "property and assets" under Article 3 of the Agreement, Article 5*quater* must be taken to imply that Equipment and Licenses "required to operate the Data Centre used by the ICRC and put in place on the premises of the Data Centre" are "property and assets". As per the definition of Equipment and Licenses in Article 1(c) of the Agreement discussed above, this includes both tangible devices, such as servers, and intangible services, specifically virtual private networks (VPNs). As the provision does not require that the ICRC be the legal proprietor of Equipment and Licenses, Article 5*quater* also applies to the aforementioned assets if they are, for example, rented by the ICRC.

As concerns Equipment and Licenses outside the Data Centre (such as servers at the ICRC's physical representation in Luxembourg), as well as data and Data and Information Systems, the Agreement does not contain a provision equivalent to Article 5*quater*. Yet, the definitions of Data and Information Systems and

47 The provision reads in full: "The property and assets of the ICRC, wherever located and by whomsoever held, shall be equally inviolable and immune from search, requisition, confiscation, expropriation or any other form of interference, whether by executive, judicial, administrative or legislative action. In particular, Luxembourg shall refrain from interfering with the ICRC's premises, property and assets by cyber means".

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

Equipment and Licenses contained in the Agreement and outlined above themselves use the term "assets", which would suggest that it is permissible to conceive of Data and Information Systems and other Equipment and Licenses as "assets". It is also worth recalling that pursuant to the definitions within the Agreement, the term "Data and Information Systems" includes "data processed and stored" in those Systems. This also brings data within the ambit of "assets".

The fact that Article 5*quater* solely mentions Equipment and Licenses within the Data Centre does not militate against this: the provision is modelled on Article 5 of the agreement between Luxembourg and Estonia which specifically governs the "hosting of data and information systems" as per its very title. One might therefore argue that the legal protection of any potential equipment and licenses outside the data centre used by Estonia is simply not addressed in the agreement governing Estonia's digital embassy in Luxembourg, rather than excluded from the scope of "property and assets". If this is so, Article 5*quater* of the Agreement between the ICRC and Luxembourg must not be understood in a limiting sense, but as a clarification that Equipment and Licenses in the Data Centre are "assets" of the ICRC in addition to Equipment and Licenses at the premises of the ICRC's physical representation. Indeed, it does not follow from this provision that "assets" excludes other Equipment and Licenses outside the Data Centre – or any data or Data and Information Systems. This understanding is further corroborated by the fact that Article 4(2) of the Agreement refers to "property and assets wherever located and by whomsoever held". In the context of the UN, this notion has been interpreted to the effect that property and assets need not be within an IO's premises to be protected by privileges and immunities.[48] Conversely, where objects are located *within* an IO's premises, they must all the more be protected by inviolability.

Importantly, it also follows from the above that intangible objects, such as data and VPNs, can constitute "assets". While this echoes the practice particularly of the UN,[49] the legal reasoning underpinning this conclusion requires further unpacking.

The notion of "property and assets" is not usually defined in instruments granting privileges and immunities to IOs, nor do the *travaux préparatoires* of the General Convention provide any insights into the meaning of those terms. Reinisch and Burci suggest that the notion of "property and assets" covers objects and rights of economic value that can be owned – i.e., over which property rights in a legal sense, including intellectual property rights, pursuant to the local law applicable where the property and assets are located can be exercised.[50] Following this approach, data

48 See August Reinisch, "Jurisdictional Immunity, Immunity of Property, Funds, and Assets (Article II Section 2 1946 General Convention)", in A Reinisch (ed.), above note 24, para. 63.

49 UN Secretariat, *Comments of the United Nations Secretariat on Behalf of the United Nations System Organizations on the "Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and Non-EEA Public Authorities and Bodies" Adopted by the European Data Protection Board on 18 January 2020*, 14 May 2020, para. 38, available at: www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf.

50 A. Reinisch, above note 48, para. 62.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

and other intangible cyber-related assets could be considered an IO's "property and assets", to the extent that the IO holds intellectual property rights over them.[51]

Tsagourias and Buchan seemingly put forward a broader interpretation, asserting that in addition to ownership, control may bring intangible objects within the purview of "property and assets".[52] This wider interpretation must be supported: if ownership were the sole criterion by which to determine the scope of "property and assets", the scope of the concept of "inviolability" might be unduly narrow. This is because the legal debate on whether data can be subject to ownership rights in a legal sense is not settled, and it may be difficult to ascertain intellectual property rights.[53] Further to this, cyber infrastructure may involve tools, created through software applications, running on physical infrastructure belonging to others, as in the case of VPNs, for example. It may be difficult to assert ownership over virtual or intangible infrastructure of this type. In contrast, as highlighted above, IOs can indeed generally exercise control over data and other intangible cyber infrastructure, in the sense that it is possible for IOs to freely create, deploy, grant or exclude access rights and otherwise dispose of data and intangible cyber infrastructure, depending on their technical set-up. As such, this wider interpretation reflects the principle of functionality, as considering data and other intangible objects within an IO's control as "property and assets" brings them within the scope of inviolability, which serves to foster an IO's information security, as demonstrated above. In light of this, a wider interpretation of the terms "property and assets" whereby both intangible and tangible assets over which an IO exercises control but does not necessarily have ownership rights, as is the UN's practice and is implicit in the Agreement between the ICRC and Luxembourg, is legally defensible.

In short, even if the Agreement is not explicit on this matter, it is arguable that data and Data and Information Systems, including intangible components thereof, as well as Equipment and Licenses both within and outside the Data Centre, constitute part of "property and assets". This wide interpretation is legally defensible, as shown above. It is true that this leads to a double classification of data, Data and Information Systems, and Equipment and Licenses both as "assets" and "archives", but this is not unusual: parts of an IO's archives regularly also fall within the scope of "property" or "assets". For instance, servers which are owned by an IO and on which information is hosted might constitute both archives and property of an IO.

51 G. L. Burci, "Immunity of Property, Funds, and Assets (Article III Section 4 Specialized Agencies Convention)", in A. Reinisch (ed.), above note 24, para. 28.

52 R. Buchan and N. Tsagourias, above note 10, p. 1177. Specifically, they consider that "where an IO is able to establish ownership or control over computer networks or 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".

53 See, for instance, Paulius Jurcys *et al.*, "Ownership of User-Held Data: Why Property Law is the Right Approach", *Harvard Journal of Law and Technology Digest*, 21 September 2021, available at https://jolt.law.harvard.edu/digest/ownership-of-user-held-data-why-property-law-is-the-right-approach. See also Jeffrey Ritter and Anna Mayer, "Regulating Data as Property: A New Construct for Moving Forward", *Duke Law and Technology Review*, Vol. 16, 2018.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

Obligations stemming from inviolability in the digital era

Having discussed the scope of the concept of inviolability under the Agreement, this section analyzes how the Agreement interprets and articulates the negative and positive obligations flowing from the concept of inviolability in the context of relevant State and IO practice.

Cyber-related negative obligations

At the outset, it is helpful to recall that the concept of inviolability entails a negative obligation on the part of the host State to refrain from interference. This obligation is typically phrased so as to proscribe executive, administrative, judicial or legislative interference, and has been understood broadly, prohibiting for instance physical force on or near an IO's premises and heavy administrative processes.[54]

The Agreement between the ICRC and Luxembourg clarifies how existing obligations for the host State to refrain from interference translate into the cyber realm. Specifically, the Agreement puts forward five cyber-related interpretations of the obligation to refrain from interference.

Article 4 of the Agreement provides that "Luxembourg shall refrain from interfering with the ICRC's premises, property and assets by cyber means". Moreover, Article 6 stipulates that "archives" include all documents and data (including electronic documents), as well as all Data and Information Systems and Equipment and Licenses, which belong to or are used or held by the ICRC, wherever located, as discussed above, and that these shall be "exempt from search, requisition, attachment or execution. Luxembourg shall refrain from interfering with the ICRC's archives by executive, administrative, judicial or legislative or any other action, including by cyber means." Further to this, Article 5*bis* of the Agreement sets out that

> [n]o official or person exercising any public authority, whether administrative, judicial, military or police of Luxembourg[,] shall enter the premises of the Data Centre used by the ICRC without the prior approval of the authorised representative of the ICRC. Such approval shall be presumed in case of fire or other emergencies that require immediate protective measures and could constitute a danger for safety.

Article 7(5) of the Agreement makes clear that "ICRC communications, including in the form of data in transit, shall be inviolable and thereby free from interference, including interception". Finally, Article 9 concerns the protection of personal data and acknowledges that the ICRC processes personal data pursuant to its own rules rather than national or regional data protection legislation.[55] In what follows, each of these provisions will be discussed in turn.

54 L. Bartholomeusz, above note 24, paras 30–33.

55 Article 9 reads in full:

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

First, in clarifying that Luxembourg shall refrain from interference with the ICRC's archives, premises, and property and assets "by cyber means", Articles 4 and 6(2) of the Agreement complement the obligation to refrain from physical disturbance.[56] These provisions intend to interpret the term "interference" in light of technical advances, providing that not only physical disturbance but also interference "by cyber means" is incompatible with the ICRC's privileges and immunities. Though States and international legal scholarship have used the term "cyber means" in discourse on the application of international law in cyberspace, there exists no agreed legal definition of these terms.[57] The Agreement equally does not define the term "cyber means". Nevertheless, the notion of "interference by cyber means" can be interpreted to capture that the host State is to refrain from any activities conducted remotely against the ICRC's data or cyber infrastructure, including accessing, disrupting or altering of data, surveillance measures and other forms of digital intrusion attributable to the State. This interpretation would seem to reflect to a large extent the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Tallinn Manual) and the majority opinion voiced therein regarding the types of digital interference that are prohibited with regard to diplomatic archives.[58]

Second, by expressly providing that data forms part of the ICRC's archives, Article 6 of the Agreement makes clear that the host State has an obligation to refrain from interfering with the ICRC's data, which corresponds to the practice of the UN.[59]

1. The processing of personal data by the ICRC shall be covered by the privileges and immunities foreseen in the present Agreement. In particular, the ICRC processes personal data in accordance with the ICRC Rules on Personal Data Protection; the ICRC's data processing is supervised by the ICRC Data Protection Office; and an effective remedy is ensured through the ICRC Independent Data Protection Control Commission.
2. The processing of data necessary to enable the ICRC to perform its humanitarian mandate established in the Geneva Conventions of 1949 and [their] Additional Protocols of 1977, to which Luxembourg is a Party, and the Statutes of the International Red Cross and Red Crescent Movement adopted by the Resolution of the International Conference of the Red Cross and Red Crescent, shall be deemed to be carried out for important grounds of public interest.
3. The ICRC shall exclusively ensure the respect of and be able to demonstrate compliance with ICRC Rules on Personal Data Protection for its processing activities, including by its processors and sub-processors as far as the ICRC is the controller.

56 Article 4 is referenced in the above subsection entitled "Data and Cyber Infrastructure as Property and Assets?". Article 6(2) reads in full: "The archives shall be exempt from search, requisition, attachment or execution. Luxembourg shall refrain from interfering with the ICRC's archives by executive, administrative, judicial or legislative or any other action, including by cyber means".

57 See, for instance, Sweden, *Position Paper on the Application of International Law in Cyberspace*, July 2022, p. 2; Costa Rica, *Costa Rica's Position on the Application of International Law in Cyberspace*, para. 2, available at: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Costa_Rica_-_Position_Paper_-_International_Law_in_Cyberspace.pdf.

58 Tallinn Manual, above note 4, p. 213. Note also that the Tallinn Manual clarifies that archives "are free from seizure, cyber espionage, enforcement, or judicial action, or any other form of interference by a State. The purpose of this protection is to ensure confidentiality." *Ibid.*, pp. 213, 215.

59 UN Secretariat, above note 49, para. 37.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

Third, turning to the protection of Data Centres, Article 5*bis* of the Agreement provides for the inviolability of any Data Centre used by the ICRC, with Article 5*bis*(2) specifying that the Luxembourg authorities must not enter the Data Centre without the ICRC's prior approval. Yet, "[s]uch approval shall be presumed in case of fire or other emergencies that require immediate protective measures and could constitute a danger for safety". The rationale behind this presumed consent is that a fire or other emergency destroying servers in a data centre can have important consequences: data centres usually contain servers processing data of a significant number of individuals and organizations, which might be destroyed, combined with the fact that ICRC staff may not always be present to detect and/or handle the emergency. It is therefore necessary to enable swift action in these circumstances. A number of instruments subject the inviolability of premises to similar presumptions of consent in cases of emergency.[60] This presumption is therefore not *per se* novel, though it is worth emphasizing that Article 4(1) of the Agreement, providing for the inviolability of premises, does not contain any similar caveat on presumed consent.[61]

Fourth, Article 7(1) of the Agreement provides that the ICRC may use freely and without interference the means of communication it deems appropriate,[62] and Article 7(5) specifies that "ICRC communications, including in the form of data in transit, shall be inviolable and thereby free from interference, including interception". This is to clarify that the obligation of non-interference applies equally to data in transit within the territory of Luxembourg and on State-controlled infrastructure. From a conceptual viewpoint, it may be considered that the protection of data in transit fits more neatly within Article 7 of the Agreement, which concerns communications of the ICRC more broadly, even if the Tallinn Manual stipulates that "both the receiving and third States are prohibited from intercepting the electronic communications of diplomatic missions and consular posts that are in transit" within the context of inviolability of archives.[63] Generally, Articles 7(1) and (5) are modelled on

60 Note that in relation to the Convention on Specialized Agencies, above note 17, it has been argued that there is an increase in headquarter agreements providing for the presumption of consent to enter premises in case of emergencies. See Riccardo Pavoni, "Inviolability of Premises (Article III Section 5 Specialized Agencies Convention)", in A. Reinisch (ed.), above note 24, para. 19.

61 Article 4(1) reads in full: "The premises of the ICRC by whomsoever they may be owned, shall be inviolable".

62 The provision reads in full: "The ICRC shall be free to use, for official purposes and without any interference, the means of communication it deems most appropriate, including messages in code, cipher or otherwise encrypted, particularly when communicating with ICRC headquarters in Geneva and its offices around the world, with other international agencies and organizations, with government departments, and with bodies corporate or private individuals. This includes all communications and data flows to or from the ICRC Cyber Infrastructure, as well as all communications and data flows processed on behalf of the ICRC through third parties in the territory of Luxembourg".

63 Tallinn Manual, above note 4, p. 221. Article 7 reads in full:

> 1. The ICRC shall be free to use, for official purposes and without any interference, the means of communication it deems most appropriate, including messages in code, cipher or otherwise encrypted, particularly when communicating with ICRC headquarters in Geneva and its offices around the world, with other international agencies and organisations, with government departments, and with

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

Article III, Sections 9 and 10 of the General Convention on communications facilities, and seek to carve out what communications facilities ought to be granted to the ICRC in the cyber era.

Fifth, Article 9 reflects the practice of the ICRC and other IOs to apply their own data protection rules, to the exclusion of national or supranational legislation, in this case the EU's General Data Protection Regulation (GDPR).[64] The UN has specifically asserted that any requirement to comply with the GDPR would be incompatible with the prohibition against interfering with the UN's data stemming from Article II, Section 3 of the General Convention, providing, *inter alia*, that the property and assets of the UN are immune from legislative interference, and Article II, Section 4 of the General Convention, whereby the archives of the UN are inviolable.[65] Echoing this legal reasoning, Article 9(1) of the Agreement clarifies that the ICRC applies only its own regulatory framework.

Article 9(2) of the Agreement clarifies that any data processing, including transfers, by entities covered by the domestic laws of Luxembourg, necessary to enable the ICRC to perform its humanitarian mandate, is considered lawful, since it is deemed to be carried out for important grounds of public interest, a legal basis for personal data processing and a derogation allowing transfers under the GDPR.[66]

Finally, Article 9(3) of the Agreement provides that, where the ICRC is the controller of personal data and engages external processors and sub-processors to process data on its behalf, the ICRC "shall exclusively ensure the respect of and be able to demonstrate compliance with ICRC Rules on Personal Data Protection". This

bodies corporate or private individuals. This includes all communications and data flows to or from the ICRC Cyber Infrastructure, as well as all communications and data flows processed on behalf of the ICRC through third parties in the territory of Luxembourg.

2. The ICRC shall have the right to purchase and install on its premises all types of telecommunication equipment and to use mobile equipment, including satellite and tracking devices, within the national territory. However, the purchase and installation of satellite and tracking devices within the national territory require prior notification by the ICRC to Luxembourg.
3. To the extent necessary to provide services to the ICRC, the ICRC shall use the frequencies assigned to it for this purpose by the competent national authority, in accordance with relevant international instruments, including Resolution No. 10 (Rev.WRC-2000) of the International Telecommunication Union.
4. In all matters relating to official communications, the ICRC shall enjoy treatment not less favourable than that accorded to intergovernmental organisations or diplomatic missions.
5. ICRC communications, including in the form of data in transit, shall be inviolable and thereby free from interference, including interception.
6. The ICRC shall have the right to dispatch and receive correspondence or any other documents, data or items by courier or in sealed bags, which shall have the same immunities and privileges as diplomatic courier and bags, provided these couriers and bags bear visible external marks of their character and contain only documents, data or items intended for official use.

64 Regulation (EU) 2016/679 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 14 April 2016 (entered into force 25 May 2018).

65 UN Secretariat, above note 49, paras 37–39. See also M. Marelli, above note 19.

66 Questions relating to the interaction between the international and domestic legal orders with regard to the applicability of domestic laws of host countries to IOs are analyzed in detail in M. Marelli, above note 19.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

provision is intended to address concerns as to possible interference with the independence of the IO by domestic laws, by virtue of such laws applying to processors of IOs.

With the foregoing provisions, the Agreement puts forward legal interpretations to clarify the negative prong of the concept of inviolability in the digital era. Yet, for purposes of comprehensiveness, a provision in the Agreement needs to be discussed which is *related to* but separate from the concept of inviolability and thus does not constitute an interpretation of obligations flowing from inviolability in the digital age. The Agreement between the ICRC and Luxembourg in effect assimilates staff of service providers, in some circumstances, to experts of the IO, who enjoy functional immunity. Article 1(g) defines "experts" broadly, encompassing "any individual providing services to the ICRC under contractual arrangements between the individual and the ICRC or between an entity and the ICRC". Article 16*bis* grants a very limited immunity to those experts, ensuring that they cannot be required to disclose information obtained in the course of their activities for the ICRC. Thus functional in nature, this immunity cannot be misused to shield individuals from accountability for misconduct; moreover, the ICRC can waive this immunity per Article 19(2) of the Agreement. This provision must be seen against a backdrop in which, as was highlighted above, leveraging digital services often requires the involvement of third parties. Software maintenance and support in many instances is carried out by third-party service providers, and data, particularly in a cloud environment, is often sub-processed by manifold entities. It cannot be excluded that service providers and hence their staff have access to the contents of IOs' data in those circumstances. The limited personal immunity of service provider staff is thus intended to reinforce host State obligations related to the inviolability of ICRC archives, cyber infrastructure and Data Centres, and constitutes a corollary of the obligation to refrain from interference with data as part of archives "wherever located".

Cyber-related positive obligations

It is worth recalling that inviolability also entails positive obligations on the part of the host State to protect against interference by the host State, as well as certain interference by third parties. In interpreting these obligations in the context of the digital era, the Agreement clarifies positive obligations in three respects.

Protection of data centres

First, the Agreement addresses the level of protection of the portions of Data Centre buildings which Luxembourg provides to the ICRC. Specifically, Article 5*ter* provides that

> [w]here the Data Centre used by the ICRC is provided by Luxembourg, the latter shall take all appropriate measures to protect the Data Centre used by the ICRC

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

> against any intrusion or damage within the territory of Luxembourg. The measures are considered appropriate if they meet the same level of protection as the protection that Luxembourg affords its own data centres.

Modelled on Article 4 of the agreement between Luxembourg and Estonia, this provision is only applicable to any government-provided Data Centre, as the Luxembourg authorities may not be able to provide the same level of protection to a commercial Data Centre.

Bilateral agreements for the exchange or provision of data in the framework of prevention, investigation, detection or prosecution of criminal offences

Second, Article 10 of the Agreement requires that

> [s]hould Luxembourg negotiate and enter into agreements with other States for the exchange or provision of data in the framework of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, Luxembourg will commit to clearly indicating that ICRC data covered by this Agreement [is] outside the scope of such agreements.

This provision must be seen against the following backdrop: recent years have seen the proliferation of legislations which authorize States to enter into agreements with other States whereby a State Party may legally require digital service providers, such as cloud service providers, under the other State Party's jurisdiction to provide a customer's data for purposes of criminal proceedings or national security. The aim of these legislations is to bypass lengthy mutual legal assistance proceedings, whereby the State which has jurisdiction over the service provider itself obtains the data and passes it on to the other State.[67] Whilst the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act), enacted in March 2018,[68] is a prominent example, other States have followed suit in adopting similar legislations, such as the UK with the Crime (Overseas Production Order) Act, and Australia with the International Production Orders Amendment to its Telecommunications Act. At the time of writing, at least two such agreements have been signed, namely between the United States and the UK, and the United States and Australia.[69]

These legislations are problematic for the ICRC, as its data could potentially be relevant to criminal proceedings and/or national security. The ICRC's data

67 See e.g. US Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law around the World: The Purpose and Impact of the CLOUD Act*, white paper, June 2019, p. 3, available at: www.justice.gov/opa/press-release/file/1153446/download.

68 See 18 US Code §§ 2713, 2523.

69 Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019 available at: www.justice.gov/criminal/file/1076581/; Agreement between the Government of Australia and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, 15 December 2021, available at: www.homeaffairs.gov.au/nat-security/files/cloud-act-agreement-signed.pdf

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

(or that of IOs more generally) is not expressly exempted from the scope of such legislations, nor any of the agreements that States have so far concluded under them. As laid out above, privileges and immunities, including inviolability of data, apply to data processed by third parties. It is also true that if at least one State has granted the ICRC adequate privileges and immunities, and particularly inviolability of archives, it is arguable that it has an obligation to prevent another State from accessing the ICRC's data. However, there are several obstacles to ensuring the effectiveness of privileges and immunities in practice. First, there may be a lack of awareness of privileges and immunities amongst officials requesting disclosure. Moreover, some of the said legislations allow States to impose non-disclosure obligations on the service provider.[70] In that case, the service provider is legally obliged to refrain from disclosing to the customer (the ICRC) that a disclosure request was made. As such, the ICRC might not be aware of the disclosure request, and might therefore not be in a practical position to protest against such a request through its usual channels, particularly by contacting the relevant ministry of foreign affairs. Equally, even if the ICRC had knowledge of such a disclosure request, some legislations do not allow challenges to a request unless the request is inconsistent with the agreement under which it was made.[71] Therefore, if an agreement between two States concluded under the CLOUD Act or similar legislation does not clarify that data of the ICRC or IOs more generally falls outside the scope of such an agreement, or if such an agreement does not state that it is without prejudice to the privileges and immunities granted to IOs or other international legal obligations that the States have undertaken, it may be difficult for the ICRC to challenge a request addressed to a service provider to disclose the ICRC's data. Clarifying that data of the ICRC or IOs more broadly falls outside the scope of such a CLOUD Act agreement would ensure that the agreement could not be used as a legal basis to request ICRC data – or that of other IOs.

In short, Article 10 of the Agreement seeks to mitigate practical obstacles to ensuring the effectiveness of privileges and immunities with a view to CLOUD Act-like legislations, and it is this rationale that underpins the requirement that ICRC data is outside the scope of agreements concluded by Luxembourg which allow another State to directly request Luxembourg service providers to disclose data.

Cooperation of Luxembourg with the ICRC in case of adverse cyber operations

Third and finally, Article 11 of the Agreement provides for cooperation of Luxembourg with the ICRC in the anticipation, prevention and attribution of, and response to, adverse cyber operations. Specifically, this provision requires Luxembourg, to the extent that it has the requisite knowledge, to provide the ICRC with certain information relating to cyber operations directly or indirectly adversely

70 See e.g. 18 US Code §§ 2703(b), 2705.

71 See e.g. Telecommunications Legislation Amendment (International Production Orders) Act, 23 July 2021, Section 121.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

affecting ICRC Cyber Infrastructure, thus comprising government-provided and/or commercial Data Centres, data, and Data and Information Systems, as well as Equipment and Licenses both in Data Centres and at the ICRC's physical delegation.[72] Several elements of Article 11 require clarification.

First, it is noteworthy that the provision refers to cyber operations adversely affecting, directly or indirectly, ICRC Cyber Infrastructure. The Cambridge Dictionary defines the term "affecting" as "to have an influence on someone or something",[73] and the notion of "affecting" is thus broader than "targeting". As such, ICRC Cyber Infrastructure need not have been the target of the cyber operation – that is, the cyber operation need not have been directed against ICRC Cyber Infrastructure. Rather, it suffices if the cyber operation has a negative impact on ICRC Cyber Infrastructure, as defined in the Agreement. Further to this, the provision also applies in certain cases of cyber operations affecting ICRC Cyber Infrastructure which are attributable to third parties.[74]

Second, the obligations that Luxembourg owes under Article 11 primarily revolve around the provision of information to the ICRC with regard to actual or potential cyber threats or operations that may adversely affect, directly or indirectly, ICRC Cyber Infrastructure as defined in the Agreement. Thus, Article 11 does not address whether the host State also has an obligation to actively prevent and terminate a cyber operation against or affecting ICRC Cyber Infrastructure, beyond the

72 The provision reads in full:

1. If Luxembourg becomes aware of new trends concerning threats, including new types of malware and nefarious cyber operations that may affect adversely directly or indirectly the ICRC Cyber Infrastructure, Luxembourg, to the extent it has requisite knowledge, shall notify the ICRC of such threats without undue delay.
2. If Luxembourg becomes aware that the ICRC Cyber Infrastructure is about to or is being adversely affected, directly or indirectly, by a cyber operation, Luxembourg shall notify the ICRC of the operation without undue delay.
3. If the ICRC Cyber Infrastructure has become subject to a cyber operation adversely affecting the ICRC directly, Luxembourg shall provide the ICRC with the information about this cyber operation available to it.
4. The scope of the cooperation is limited to the ICRC Cyber Infrastructure hosted on the territory of Luxembourg.
5. A procedure for the exchange of information shall be established and implemented in a subsequent agreement in respect of the potentially sensitive nature of the information shared, of national and international agreements, and in compliance with national and European Union legislation. Any exchange of information on the part of ICRC is subject to its standard working modality of confidentiality.

73 "Affect", *Cambridge Dictionary*, available at: https://dictionary.cambridge.org/dictionary/english/affect#google_vignette.

74 See further, on host State obligations relating to interference by third parties, ILC, *Report to the General Assembly*, UN Doc. A/CN.4/SER.A/1957/Add.1, 1957, in *Yearbook of the International Law Commission*, Vol. 2, 1957, Documents of the Ninth Session including the Report of the Commission to the General Assembly, p. 137. See also ICJ, *Tehran*, above note 42, para. 66, wherein the Court notes the absence of any "apparent steps either to prevent the militants from invading the Embassy or to persuade or to compel them to withdraw". Further, see paras 67–68, wherein the Court clearly finds that Iran's inaction in the face of the intrusion and other acts by non-attributable third parties "by itself" constituted a clear and serious violation of Iran's obligations, particularly under the VCDR.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

provision of information. The purpose of Article 11 is to clarify merely one prong of the wider obligation to protect the ICRC's data and Cyber Infrastructure within the broader purview of the inviolability of archives and property and assets.

The UN has explicitly asserted that "States, and in particular host countries, have a duty to protect organizations from hostile attacks, whether in the physical or in the digital sphere",[75] but it has refrained from expanding on the precise measures required of host States. Presumably, this ambiguity is due to the fact that the exact measures to be taken by the host State may vary depending on the nature and scale of any particular cyber operation to which the IO may be subject. Similarly, the Tallinn Manual requires a receiving State to take steps to prevent or terminate cyber operations targeting (rather than merely affecting) the cyber infrastructure of a diplomatic mission.[76]

The omission in the Agreement of any explicit reference to any obligation to actively prevent or terminate cyber operations needs to be seen against the following backdrop, as noted by Marelli:

> Because of its control over the network on its territory and flows of data going through it, the resources and expertise available, and the international cooperation networks it is likely to be involved in, a cyber host State may have much better means than the organization alone to anticipate, detect, attribute and respond to cyber operations. Defining the perimeters of this dialogue will be a very sensitive task and will be important in order to ensure that, on the one hand, the dialogue is effective, while, on the other hand, it does not make the organization over-reliant on the cooperation of the cyber host State, thereby creating a risk that the neutrality, impartiality and independence of the organization will be compromised.[77]

These difficulties in striking a balance between the host State's advanced capability in the digital sphere and the need for the ICRC's independence in cyberspace and the digital age is what differentiates cyber operations against ICRC Cyber Infrastructure from physical interference with, for instance, ICRC offices, such as robberies. With regard to physical interference with physical objects, decades of practice exist to clearly outline expectations on the host State and delineate protective measures acceptable for the ICRC, while cyber threats are comparatively novel. As such, Article 11, and the language in the Agreement more broadly, ensures cooperation and support from the host State with regard to the protection of the ICRC's data, Cyber Infrastructure and Data Centres without affecting the ICRC's neutrality and independence.

In a similar vein, the Agreement indirectly addresses the possibility of the host State taking countermeasures in response to a cyber operation which adversely

75 *Cybersecurity in the United Nations System Organizations*, above note 35, para. 5.

76 See Tallinn Manual, above note 4, p. 217.

77 M. Marelli, above note 8, p. 384.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

affects the ICRC.[78] Particularly without the ICRC's consent, any countermeasures in response to a cyber operation affecting the organization remain an act of a State.[79] Nevertheless, even where countermeasures are not attributable to the ICRC, the State subject to those countermeasures may *perceive* the ICRC's neutrality to be affected, and, for instance, may limit the ICRC's access to affected persons. It is against this backdrop that Article 20 of the Agreement must be read in requiring that "[a]ny interpretation of international law provisions affecting the ICRC, including in cyber operations, shall be driven by the respect of the ICRC's impartiality, neutrality, and independence". This provision recognizes that it is the host State's prerogative to interpret its sovereignty, call on due diligence or take countermeasures, whilst leaving space to accommodate considerations relating to the ICRC's steadfast neutrality.

Finally, it should be noted that the Agreement also leaves some questions open and requires the parties to define certain procedures separately. In particular, in relation to the cooperation of Luxembourg with the ICRC in relation to actual or potential cyber operations, Article 11(5) stipulates that

> a procedure for the exchange of information shall be established and implemented in a subsequent agreement in respect of the potentially sensitive nature of the information shared, of national and international agreements, and in compliance with national and [EU] legislation. Any exchange of information on the part of [the] ICRC is subject to its standard working modality of confidentiality.

In short, with the aforementioned provision, the Agreement seeks to flesh out some elements of the positive prong of the concept of inviolability.

Conclusion

The Agreement between the ICRC and Luxembourg provides holistic protection of the ICRC's data, Data Centres and Cyber Infrastructure from unauthorized access by putting forward legal interpretations of the scope of inviolability, and positive and negative obligations flowing from inviolability, which are in line with the principle of functionality and reflect to a large extent existing State and IO practice. The practical effect of these interpretations is reinforced by the limited functional immunity of certain third-party service provider staff – an obligation separate from the concept

78 On countermeasures in cyberspace, see e.g. Talita Dias, *Countermeasures in International Law and Their Role in Cyberspace*, Chatham House International Law Programme Research Paper, May 2024, available at: www.chathamhouse.org/sites/default/files/2024-05/2024-05-23-countermeasures-international-law-cyberspace-dias.pdf

79 See ILC, *Draft Articles on the Responsibility of International Organizations*, 2011, Art. 9, whereby "[c]onduct which is not attributable to an international organization under articles 6 to 8 shall nevertheless be considered an act of that organization under international law if and to the extent that the organization acknowledges and adopts the conduct in question as its own". On multiple attribution or "shared responsibility", see André Nollkämper *et al.*, "Guiding Principles on Shared Responsibility in International Law", *European Journal of International Law*, Vol. 31, No. 1, 2021.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press

of inviolability. Overall, the Agreement constitutes an essential contribution to the ICRC's information security, and thus to its ability to be a neutral, independent and impartial humanitarian actor, and to observe its working modalities of confidentiality and "do no harm" in an ever more digitalized world. The Agreement thus reflects how inviolability should be interpreted to give the ICRC the tools to do its job in the digital era.

https://doi.org/10.1017/S1816383125000190 Published online by Cambridge University Press