# Internet and eDiplomacy: 'Traditional' Diplomatic Law in the Digital Era

Stefano Dominelli*
University of Genoa, Genoa, Italy
*stefano.dominelli@unige.it*



## Abstract

The rise of internet and social media has changed, amongst others, international politics and international relations, putting the rules of the 1961 Vienna Convention on Diplomatic Relations under a stress test. The present work wishes to contribute to the current scholarly debate on whether already existing traditional rules of diplomatic law can easily be adapted to a post-modern world.

More in detail, it will be dwelled if and to what extent diplomatic privileges and immunities conceived for an 'in person' diplomacy can be applied to 'eDiplomacy' as well. The proper identification of notions such as 'premises', 'archives', or 'correspondence' are currently under debate, as is the regime of protection of diplomatic premises in cases of cyber-crimes. Additionally, at current times, it seems the most prominent issue relates to the possibility to use in court diplomatic protected documents illegally obtained. Under the 1961 Vienna Convention, it remains unclear whether an unlawfully obtained diplomatic cable is always inadmissible. More straightforward seem to be other issues of eDiplomacy, either because the existing legal framework appears sufficiently flexible to be interpreted in such a way as to cope with eDiplomacy, or because international diplomatic law is not applicable to such new scenarios, leaving the door open for States to elaborate original solutions, if they deem it opportune.

* Researcher in International Law, University of Genoa.

DOI 10.17104/0044-2348-2021-3-733 ZaöRV 81 (2021), 733-753

## Keywords

Diplomatic Law – VCDR – diplomatic online communications – online diplomatic privileges

# I. Introduction

The 'digital revolution' has brought significant societal changes in many countries of the world.[1] Legal narratives have evolved accordingly over time, exploring and unravelling topical issues[2] as there appear to be few areas of

1 On the internet as one of the tools for social change, see *ex multis* Miriyam Aouragh and Anne Alexander, 'The Egyptian Experience: Sense and Nonsense of the Internet Revolution', International Journal of Communication 5 (2011), 1344-1358; on the efforts by States to 'control' the internet and limit its impact amongst the masses, see Kal Raustiala. 'Governing the Internet', AJIL 110 (2016), 491-503. Specifically on the control over the internet in China, see Katherine Tsai, 'How to Create International Law: The Case of Internet Freedom in China', Duke J. Comp. & Int'l L. 21 (2011), 401-430.

2 On territorial sovereignty in the digital era, see Martti Koskenniemi, 'What Use for Sovereignty Today?', Asian Journal of International Law 1 (2011), 61-70; Henry H. Jr. Perritt, 'The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance', Ind. J. Global Legal Stud. 6 (1998), 423-442 (425 ff.); Patrick W. Franzese, 'Sovereignty in Cyberspace: Can it Exist?', A. F. L. Rev. 64 (2009), 1-42; Benedikt Pirker, 'Territorial Sovereignty and Integrity and the Challenges of Cyberspace' in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallin: NATO CCD COE Publication 2013), 189-216; Wolff Heintschel von Heinegg, 'Territorial Sovereignty and Neutrality in Cyberspace', International Law Studies 89 (2013), 123-156; and Nicholas Tsagourias, 'The Legal Status of Cyberspace' in: Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar 2015), 13-29 (17 ff.); on warfare approaches and artificial intelligence see Michael W. Lewis and Emily Crawford, 'Drones and Distinction: How IHL Encouraged the Rise of Drones', Geo. J. Int' l L. 44 (2013), 1127-1166; Chantal Grut, 'The Challenge of Autonomous Lethal Robotics to International Humanitarian Law', Journal of Conflict and Security Law 18 (2013), 5-23; Marco Sassòli, 'Autonomous Weapons and International Humanitarian Law: Advantages, Open Technical Questions and Legal Issues to be Clarified', International Law Studies 90 (2014), 308-340; Markus Wagner, 'The Dehumanization of International Humanitarian Law: Legal, Ethical, and Political Implications of Autonomous Weapon Systems', available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2541628>; Kjølv Egeland, 'Lethal Autonomous Weapon Systems under International Humanitarian Law', Nord. J. Int'l L. 85 (2016), 89-118; Alan L. Schuller, 'At the Crossroads of Control: The Intersection of Artificial Intelligence in Autonomous Weapon Systems with International Humanitarian Law', Harvard National Security Journal 8 (2017), 379-425; on online hate speech see Joseph Rikhof, 'Hate Speech and International Criminal Law: The Mugesera Decision by the Supreme Court of Canada', JICJ 3 (2005), 1121-1133; Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law', Max Planck UNYB 10 (2006), 191-272; James Banks, 'European Regulation of Cross-Border Hate Speech in Cyberspace: The Limits of Legislation', European Journal of Crime, Criminal Law and Criminal Justice 19 (2011), 1-13; Federica Falconi, 'Addressing Disability Hate Speech: The Case for Restricting Freedom of Expression in the Light of

 DOI 10.17104/0044-2348-2021-3-733

human activities – and, consequently, branches of law – that are left unaffected by the development of information technology.

International diplomatic (and consular) law is no exception. A greater possibility to make recourse to computer-based resources in diplomacy[3] changes the way foreign politics is expressed and international diplomacy is conducted. Recourse to social media by (some) Heads of States and politicians can increase the level of public participation in the decision-making

---

the ECtHR's Case Law' in: Carola Ricci (ed.), *Building an Inclusive Digital Society for Persons with Disabilities New Challenges and Future Potentials* (Pavia: Pavia University Press 2019), 69-81; on access to internet as a fundamental right see Steven Hick, Edward F. Halpin and Eric Hoskins (eds), *Human Rights and the Internet* (New York: Palgrave 2000); and Stephen Tully, 'A Human Right to Access the Internet? Problems and Prospects', HRLR 14 (2014), 175-195; and on private international law in the digital world see Anna Gardella, 'Diffamazione a mezzo stampa e Convenzione di Bruxelles del 27 settembre 1968', Rivista di diritto internazionale privato e processuale 3 (1997), 657-680; Manlio Frigo, 'Recognition and Enforcement of Judgments on Matters Relating to Personality Rights and the Recast of the Brussels I Regulation' in: Fausto Pocar, Ilaria Viarengo and Francesca C. Villata (eds), *Recasting Brussels I* (Milan: CEDAM 2012), 341-352; Susanne L. Gössl, *Internetspezifisches Kollisionsrecht? – Anwendbares Recht bei der Veräußerung virtueller Gegenstände* (Baden-Baden: Nomos 2014); Alex Mills, 'The Law Applicable to Cross-Border Defamation on Social Media: Whose Law Governs Free Speech in "Facebookistan"?', Journal of Media Law 7 (2015), 1-35; Giovanni Zarra, 'Conflitti di giurisdizione e bilanciamento dei diritti nei casi di diffamazione internazionale a mezzo Internet', Riv. Dir. Int. 98 (2015), 1234-1262; Dan Jerker B. Svantesson, *Private International Law and the Internet* (Alpeen aan den Rijn: Wolters 2016); Simone Carrea, 'L'individuazione del forum commissi delicti in caso di illeciti cibernetici: alcune riflessioni a margine della sentenza Concurrence Sàrl', Diritto del commercio internazionale 31 (2017), 543-571; and Tobias Lutzi, *Private International Law Online* (Oxford: Oxford University Press 2020).

3 For example, for the purposes of increased capacities of direct communication between States without the necessity of the intermediation of diplomatic staff; enhanced capacity to collect relevant information over the internet with smaller sized permanent missions abroad; direct communication between nationals and (long distant) consular posts over email; to update communication channels between the sending State and its missions abroad; to organise pre-negotiations phases in bilateral or multilateral conferences or to possibly establish 'virtual diplomatic missions abroad' (as in the case of the US virtual Embassy in Iran in 2011, whose website was blocked for several hours by local authorities), see The White House, Office of the Press Secretary, Statement by the Press Secretary on Iran's Blockage of Virtual Embassy Tehran, 7 December 2011, available at <https://obamawhitehouse.archives.gov>; Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge, Cambridge University Press 2017), 216; and Eytan Gilboa, 'Digital Diplomacy', in Costas M. Constantinou, Pauline Kerr and Paul Sharp (eds), *The SAGE Handbook of Diplomacy* (London: Sage 2016), 540-551 (544); on the greater recourse to IT in diplomacy, see *ex multis* Won-Mog Choi, 'Diplomatic and Consular Law in the Internet Age', Singapore Yearbook of International Law 10 (2006), 117-132 (118 ff.); Holger P. Hestermeyer, 'Vienna Convention on Diplomatic Relations (1961)' in Rüdiger Wolfrum (ed.), *MPEPIL* (Oxford: Oxford University Press 2009), 697-709, paras 28 and 43; Jovan Kurbalija, 'The Impact of the Internet and ICT on Contemporary Diplomacy' in: Pauline Kerr and Geoffrey Wiseman (eds), *Diplomacy in a Globalizing World. Theories and Practices* (Oxford: Oxford University Press 2013), 141-150; and Jovan Kurbalija, 'E-Diplomacy and Diplomatic Law in the Internet Era' in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy* (Tallin: NATO CCD COE Publication 2013), 393-424.

DOI 10.17104/0044-2348-2021-3-733 ZaöRV 81 (2021)

process with potentially positive effects on the democratic legitimacy of diplomacy and online negotiations may turn out less adversarial than *de visu* meetings.[4] Of course, for 'eDiplomacy' to remain and flourish in the field of international relations and diplomacy, the legal framework should be as clear and predictable as possible. As it will be argued, this is not necessarily the case. Commenting some events that have taken place in recent years,[5] the aim of this paper is to explore the persistent relevance of the main international treaties in the field of diplomatic relations contextualised in the framework of eDiplomacy. In other words, the paper aims to put the current international diplomatic law to a 'stress-test' and analyse if and to what extent emerging practices may be regulated by one of the most traditional branches of international law. By combining positivism and a policy-oriented approach, the present work will seek to reconstruct what is the law mainly under the 1961 Vienna Convention on Diplomatic Relations (VCDR)[6] and the 1963 Vienna Convention on Consular Relations (VCCR)[7] where electronic tools and resources have already been employed in the field of diplomatic law, to understand if and to what extent 'traditional' international diplomatic law is flexible enough to cope with the main current digital challenges. The overall argument will be that, despite some difficulties in terms of qualification of new 'scenarios' for the purposes of the applicability of the Vienna Conventions, such treaties remain a valid text. However, this does not mean that the conventions remain a good-for-all legal framework. Some questions may be

4 Stressing the consequences of 'secrecy' connected to e-negotiations, as 'A negotiation process made in through such tools would become less visible to the public and thus the decision-making would be done without much pressure', see Paula Sullaj, 'Digitalization of Diplomacy: A New Way of Making Diplomacy?', Rivista elettronica del Centro di Documentazione Europea dell'Università Kore di Enna, available at <httpa://unikore.it>. From a practical side, whereas this might pave the way to more 'behaved' discussions in bilateral meetings (and in meetings in general), in multilateral fora, a full online negotiation does not necessarily appear fully suited to ensure the best outcome and substantive equality in terms of participation to the negotiation. Moreover, in more general terms, the less 'publicity' to the event following the online nature could run counter the idea of democratic participation to foreign policy and international diplomacy as well. In the scholarship, cf also Choi (n. 3), 119.

5 Amongst the most 'incumbent' issues of eDiplomacy, the use of social media for diplomatic purposes and the applicability of relevant rules of diplomatic law; the establishment of virtual embassies and the applicability of rules on inviolability of premises; the possibility to use in court diplomatic cables unlawfully extracted from diplomatic archives and made freely available online (on which see UK Supreme Court, *R (on the application of Bancoult No 3) (Appellant) v. Secretary of State for Foreign and Commonwealth Affairs (Respondent)*, judgment of 8 February 2018, [2018] UKSC 3), and the possibility to overrule the principle of inviolability of diplomatic premises where cyber-crimes are either emanating from or attacking an Embassy.

6 UNTS, Vol. 500, 95.

7 UNTS, Vol. 596, 261.

 DOI 10.17104/0044-2348-2021-3-733

too far away from the 'traditional' rules and their scope of application[8], whilst other practical issues that have already emerged do not appear apt to be regulated by the Vienna Conventions because they exceed the reconstructed scope of application of the treaties.[9]

## II. 'Diplomatic Communications' Through Social Media

Due to the lack of replies, the Swedish Minister for Foreign Affairs, in 2012, tweeted the Ministry of Foreign Affairs of Bahrein who – after answering to the Twitter shout-out – apparently made recourse to traditional channels for an official response.[10] High ranking officials, and some Heads of States in particular,[11] make increasing recourse to instruments such as Twitter or Facebook in their domestic and international politics. This raises the issue of the legal status of such communications. However, two different scenarios should be separately considered and addressed; on the one side, social media communications from the diplomatic corps accredited within a State, and – on the other side – social media communications made from Heads of States or Governments, and from Ministers of Foreign Affairs.

As to the first case, under international diplomatic law, 'All official business […] entrusted to the mission by the sending State shall be conducted with or through the Ministry for Foreign Affairs of the receiving State […]'.[12] At the same time, there is a principle of freedom of forms

8 For example, one of the fields where in the near future necessities for specific new rules may become urgent, is that of secrecy and data protection when diplomatic agents use third private parties applications for their reserved or secret communications (such as, e. g. Zoom or similar apps that have taken full potential out of the pandemic crisis). In this sense, it has become quite normal to see European Union videolink meetings where representative of States negotiate the content of a piece of legislation to be.

9 As may be the case for 'diplomatic communications' through social media, on which see *amplius infra*.

10 As reported by Andreas Sandre, *Twitter for Diplomats* (Lausanne: DiploFoundation and Istituto Diplomatico 2013), 28.

11 One of the most notable examples probably being Donald Trump during his terms of office as President of the United States of America, on whose recourse to Twitter and 'Twitter Diplomacy', see Constance Duncombe, 'Twitter and the Challenges of Digital Diplomacy', SAIS Review of International Affairs 38 (2018), 91-100; and Maja Šimunjak and Alessandro Caliandro, 'Twiplomacy in the Age of Donald Trump: Is the Diplomatic Code Changing?', The Information Society 35 (2019), 13-25.

12 Art. 41(2) VCDR. On which see Eileen Denza, *Diplomatic Law* (Oxford: Oxford University Press 2016), 382; and Niklas Wagner, Holger Raasch and Thomas Pröbstl, *Wiener Übereinkommen über diplomatische Beziehungen vom 18. April 1961: Kommentar für die Praxis* (Berlin: BWV Berliner Wissenschafts-Verlag 2007), 365.

DOI 10.17104/0044-2348-2021-3-733 ZaöRV 81 (2021)

for communications between the sending State and its missions abroad,[13] and the convention is generally silent on the form of communication between the Embassy and the receiving State. Diplomatic practice has in this last regard developed a wide range of forms, such as the ones explicitly regulated within given legal systems, of First-Person Notes; Note Verbale; Memorandum; Aide-Memoire; Pro Memoria; Note Diplomatique; Note Collective; and Circular Diplomatic Notes.[14] Yet, domestic laws of the receiving State may impose limitations as per the means of communication for specific acts, requiring for example a note verbale rather than other forms.

'Twitter diplomacy' from Ambassadors hardly fits established categories, and 'tweets' *may* fall within the scope of application of the VCDR only if i) communications are conducted through the Ministry of Foreign Affairs of the receiving State (Art. 42(2) VCDR); ii) if the latter does not at least prohibit 'Twitter diplomacy'; and iii) if a principle of freedom of forms can be transposed from the rules on communication between the Embassy and its State to the communication between the Embassy and the receiving State. From an historical perspective, States appear quite bound to a formalistic (and ritualistic) approach to international diplomacy, and a public tweet might be deemed to be in violation of the requirement to carry out official business 'through' the Ministry of Foreign Affairs of the receiving State. In other words, if 'tweets' *might* be acceptable under *formal* aspects, they can violate the rules concerning the *channel of communication*,[15] with the consequence that diplomatic accredited corps should refrain from using it for official purposes (unless otherwise agreed between the States). Similar issues could rise for blogs used by diplomats to inform the public of the situation within their Host State – after the authorisation of their home countries.[16] Such activity might not only breach the duty to communicate through the Ministry of Foreign Affairs of the receiving State, but it might also amount to an unduly interference with the national (domestic and international) affairs.

Perhaps more common and widespread is the recourse to social media in the last years by Heads of States or other top-ranking officials. In general

13 Art. 27(1) VCDR. See Ivor Roberts (ed.), *Statow's Diplomatic Practice* (Oxford: Oxford University Press 2009), 114.

14 On which see US Department of State, Foreign Affairs Manual and Handbook, 5 FAH-1 H-610 ff., Using Diplomatic Note, available online.

15 See Kurbalija, E-Diplomacy (n. 3), 423. See Art. 41(2) VCDR, according to which 'All official business with the receiving State entrusted to the mission by the sending State shall be conducted with or through the Ministry for Foreign Affairs of the receiving State or such other ministry as may be agreed'.

16 Denza (n. 12), 381.

 DOI 10.17104/0044-2348-2021-3-733

terms, it can preliminary be noted that, despite the many legal doubts surrounding the use of social media in international law, these have been significantly used.[17] However, the relevance of social media by Heads of States can be approached from different perspectives.

From the specific point of view of diplomatic law, the VCDR does not apply to the communication of Heads of States, regardless of the type of the communication. The treaty might nonetheless constitute a reference point at the interpretative level.[18]

For those unilateral acts which might fall within the material scope of application of diplomatic law, thus be characterised as unilateral diplomatic communications directed at other international actors, it has to be noted that State practice has developed a principle of freedom of forms. 'Recognition' of new States, and the intention to start diplomatic relationships have been communicated by various means, such as conference presses or phone calls.[19]

17 Whilst the constitutive elements of domestic practices can be drawn from a wide array of elements, caution is generally followed; see Second Report on the Identification of Customary International Law, by Michael Wood, Special Rapporteur, International Law Commission. Sixty-sixth session, 22 May 2014, A/CN.4/672, para. 29: 'All evidence must be considered in light of its context. In assessing the existence or otherwise of the two constituent elements, be it by reviewing primary evidence or by looking to subsidiary means, great care is required. While "evidence can be taken [from a variety of sources] […] the greatest caution is always necessary." Much depends on the particular circumstances in determining what the relevant practice actually is and to what extent it is indeed accepted as law, and different weight may be given to different evidence. For example, "[p]articularly significant are manifestations of practice that go against the interest of the State from which they come, or that entail for them significant costs in political, military, economic, or other terms, as it is less likely that they reflect reasons of political opportunity, courtesy, etc." In a similar manner, the care with which a statement is made is a relevant factor; less significance may be given to off-the-cuff remarks made in the heat of the moment'. See also International Law Commission, seventieth session, 2018, A/73/10, Draft conclusions on identification of customary international law, Conclusion 6(1) ('Practice may take a wide range of forms. It includes both physical and verbal acts [...]'), whose commentary reads that 'While some have argued that it is only what States "do" rather than what they "say" that may count as practice for purposes of identifying customary international law, it is now generally accepted that verbal conduct (whether written or oral) may also count as practice [...]'.

18 ICJ, *Arrest Warrant of 11 April 2000* (Democratic Republic of the Congo v. Belgium), Judgment of 14 February 2002, I. C. J. Reports 2002, 3 (para. 52).

19 On which see Carlo Curti Gialdino, *Lineamenti di diritto diplomatico e consolare* (Torino: Giappichelli 2015), 10 ff., and 68. The beginning of diplomatic relationships between the United States of America and the Holy See were announced by the respective press conferences in 1984, and in 1960 Cuba announced the establishment of diplomatic relationships with China – who was unaware of this intention but accepted and conformed accordingly. In December 2017, US President Donald Trump tweeted that 'I have determined that it is time to officially recognize Jerusalem as the capital of Israel. I am also directing the State Department to begin preparation to move the American Embassy from Tel Aviv to Jerusalem', thus showing how social media 'declarations' are followed by traditional diplomatic channels of communication, being more an 'anticipation' of subsequent possible official State positions.

If such an approach of freedom of forms for unilateral acts might have any value in the context of official social media unilateral communication, it would have to mean that, from the very specific focal lenses of diplomatic law, the nature of social media as a communication tool does not negatively affect the communication as 'diplomatic communication'. Of course – the question, whose answer is everything but straightforward – is under which conditions expressions made through social media can amount to 'unilateral declarations' under international law and are for these purposes attributable to the State and exert effects on the plane of the international community generating obligations.[20]

For bilateral acts, if the VCDR is again to offer any guidance, its underlying principle of mutual consent between States should at least suggest that State-to-State communication between Heads of States by way of social media, to be acknowledge or legally binding, should expressly be accepted as 'diplomatic means of communication'. A solution that, from a practical perspective and taken into consideration the ritualistic approach that generally permeates the field, appears unlikely at least.

Outside these boundaries, social media should not be considered as means of diplomatic communication and diplomatic law should not be considered applicable. If a social media post is not considered a legitimate means of diplomatic communication, either because international diplomatic law is not applicable or because the 'post' tweeted by the politician is destined to a domestic audience (making the act 'non-international' in nature, even though with relevance on the field of foreign policy), possible consequences of course remain open if one adopts different focal lenses of international law, such as for example the rules on the use of force.[21] The circumstance that a 'tweet' or a 'post' falls outside the scope of application of international diplomatic law does not necessarily and automatically mean that the very same social media post does not bear any relevance at all for other branches of international law.

20 Extensively, see Erlend Serendahl, 'Unilateral Acts in the Age of Social Media', Oslo Law Review 5 (2018), 126-146.

21 Serendahl (n. 20), 138-139, referring to the diplomatic ramifications of social media activity, more specifically referring to posts of President Trump directed at the US population conveying messages to North Korea, raising questions of a potential unlawful threat of the use of force in violation of Art. 2(4) UN Charter.

 DOI 10.17104/0044-2348-2021-3-733

## III. Diplomatic Premises, and 'Virtual' Embassies and Consular Posts

Some States have already established either 'virtual' Embassies or consular posts abroad. In 2007 the Maldives and Sweden opened respectively a 'full' virtual embassy and a cultural office.[22] Such embassies were 'created' within a specific webpage, *secondlife.com* – an open 3D virtual world developed by a private US company.

Other States have proceeded differently, establishing virtual embassies using governmental tools, namely official webpages of the State – such as the United States of America who did set up a virtual Embassy in Tehran in 2011. Similarly, to have some contacts with States (and their people) with whom it had no formal diplomatic relationship, Israel opened a 'Twitter Embassy account' in 2013 for the Gulf States[23], which closed soon after in 2014 and was re-launched in 2019.[24]

The advantages of virtual establishments are apparent, both in terms of economics and public administration management[25] (especially for small size States unable to establish representations in all foreign countries), and in terms of possibility to unilaterally reach foreign people and institutions where diplomatic relationships are broken. Yet, the relevant *legal* question is whether such digital tools do amount to Embassies or consular post, thus entitled to any specific protection.

From an historical perspective, the VCDR strongly rests upon a physical conceptualisation of diplomatic missions. According to its Art. 1(i), 'premises of the missions' are buildings and land.[26] The receiving State must assist the sending State in the search for necessary premises.[27] These buildings and

22 Gilboa (n. 3), 544.

23 Ilan Manor, *The Digitalization of Public Diplomacy* (Cham: Palgrave 2019), 228.

24 'Israel Re-launches "Virtual Embassy" on Twitter for Gulf Dialogue', 7 February 2019, <https://www.middleeastmonitor.com>.

25 See Dietrich Klapper, 'New Diplomatic Tools and the Broadening Access of Developing Counties' in: Justin Robertson and Maurice A. East (eds), *Diplomacy and Developing Nations: Post-Cold War Foreign Policy-making Structures and Processes* (Oxon: Routledge 2005), 80-93 (85 ff.); and Justyna Arendarska, 'Foreign Ministries in the Perspective of Information Revolution' in: Monika Szkarłat and Katarzyna Mojska (eds), *New Technologies as a Factor of International Relations* (Newcastle upon Tyne: Cambridge Scholars Publishing 2016), 91-105 (92).

26 'The "premises of the mission" are the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission including the residence of the head of the mission.' See Jean d'Aspremont, 'Diplomatic Premises' in: Rüdiger Wolfrum (ed.), *MPEPIL* (online ed., Oxford: Oxford University Press 2009), 1 ff.; Denza (n. 12), 16; and Wagner, Raasch and Pröbstl (n. 12), 53.

27 'The receiving State shall either facilitate the acquisition on its territory, in accordance with its laws, by the sending State of premises necessary for its mission or assist the latter in obtaining accommodation in some other way' (Art. 21(1) VCDR).

DOI 10.17104/0044-2348-2021-3-733 ZaöRV 81 (2021)

lands, their furnishings and other property thereon are protected from foreign intrusions, as they enjoy inviolability under Art. 22 VCDR. Even though the convention seeks an extensive definition of 'premises' – by including buildings not in property of the foreign State[28] or by including short-term rent of immovable properties destined to the diplomatic function[29] – a literal interpretation, historically contextualized, seems to point towards the idea that virtual 'Embassies' are not such in legal terms. Subsequent practice seems of little help to argue that a clear and settled customary law rule extending the definition of 'Embassies' has already emerged. Practice appears quantitatively not sufficient, as this comprises that of some Insular or Micro-States, Israel, Sweden, and the United States (US) only.

Moreover, some of these practices either show resistances in recourse to virtual posts, or theoretical inconsistencies which militate against an evolutionary interpretation in international law.

Some States, such as Sweden, have closed their 'missions',[30] whilst others – such as Israel – have had a practice inconsistent in time, intermittent, and for limited and specific purposes.

Iran did block the US virtual Embassy in Tehran, by obscuring the website.[31] The United States of America themselves disqualified their own tool by clearly stating: 'This website is not a formal diplomatic mission, nor does it represent or describe a real U.S. Embassy accredited to the Iranian Government. But, in the absence of direct contact, we hope it can serve as a bridge between the American and Iranian people'.[32]

It seems however that the question at hand cannot be given a single and unitary answer, as different scenarios require different evaluations.

The first case to be dwelled upon is that of virtual missions opened and running on privately-owned websites, such as Second Life or Twitter. It is true that under the VCDR, 'premises' are not necessarily property of the foreign State; yet, once in their possession, the foreign State acquires a significant control over the *res*, which becomes inviolable to public and private entities (with well-known issues in cases of evictions if rent is not paid). The use of private websites and social media seems inconsistent with the idea of control of the premises, as States using such accounts have no

28 D'Aspremont (n. 26), 2; Denza (n. 12), 16; and Wagner, Raasch and Pröbstl (n. 12), 54. However property alone, also if given, does not suffice to ensure application of diplomatic privileges to the building (see Roberts (n. 13), 107).

29 Wagner, Raasch and Pröbstl (n. 12), 54 f.

30 Gilboa (n. 3), 544.

31 The White House, Office of the Press Secretary, 7 December 2011, Statement by the Press Secretary on Iran's Blockage of Virtual Embassy Tehran (n. 3).

32 On the website, <https://ir.usembassy.gov>. Cfr in the scholarship, Yolanda Kemp Spies, *Global South Perspectives on Diplomacy* (Cham: Palgrave 2019), 25.

different treatment than the public. The very existence of the 'virtual mission' will depend on the policies of both the 'receiving State', who might obscure single accounts or the social media at large, and of the private company, as this could retain the faculty to 'block' the account in accordance with the terms and conditions of the contract – a 'self-enforcement' measure that is not given to tenants of the building of the mission. In this sense, due to the lack of control over the *res* inherently required by the VCDR, privately-owned websites should not be classified as 'diplomatic premises' for the purposes of diplomatic law. Consequently, no diplomatic law protection should be granted, until at least an eventual subsequent State practice to the contrary can successfully be reconstructed.

The second case which deserves some thought is that of a virtual mission running on a governmental website. Such scenario would not meet the critiques of missions relying on private systems, yet the leading principle should remain that of consent,[33] as this strongly characterizes diplomatic relations. Under the VCDR, 'The establishment of diplomatic relations between States, and of permanent diplomatic missions, takes place by mutual consent.'[34] In this sense, a 'unilateral diplomatic mission' is no diplomatic mission under diplomatic law. Hence, actions such as blocking the website of the foreign State should not constitute a violation of diplomatic law, nor a violation of the foreign State's right to enter into contact (and influence) a given population with its website (as such a right to contact and influence other populations could hardly be reconstructed).

If the concerned States do not agree anything specific on the inviolability of the website, provided that this does not amount to 'premises of the mission' under the VCDR, some of its rules might nonetheless still be applicable.[35] If the governmental website runs on servers placed at a 'physic' diplomatic mission, accredited to the receiving State, such servers should enjoy both physical and 'virtual' inviolability. The first deriving from its location inside the premises of the Embassy; the second, from the principle of avoiding unduly interferences that is embedded in the convention[36] and in general principles of public international law. However, if there is no physical reality of the website attached to diplomatic premises in the host State, i. e. where there is no diplomatic premise and the server hosting the website is in

33 See also Schmitt (n. 3), 216.

34 Art. 2 VCDR.

35 See also Schmitt (n. 3), 216.

36 Cf. Art. 37(4) VCDR, according to which the jurisdiction of the receiving State over private servants of the mission shall be exercised to the extent immunity is not granted, and provided that jurisdiction is exercised in such a manner 'as not to interfere unduly with the performance of the functions of the mission'.

its State of origin (or in a third State), as 'virtual embassies' do not fall within the scope of application of the VCDR,[37] a subsequent blockage by the State to whom it is directed would still not constitute a breach of general diplomatic law.

## IV. Diplomatic Emails and Private 'Inter-Net-Ferences'

In the context of online communication and online storage systems used for diplomatic purposes,[38] the *Bancoult 3*[39] judgment of the United Kingdom Supreme Court (UKSC) is one of the most recent cases[40] showing the complexities and limits surrounding the VCDR in relation to 'internet cases'. The issue concerned 'The leaking of governmental documents and their widespread distribution through the internet', which 'is a phenomenon of our time. The status of leaked documents in the public domain is an issue which is likely to recur'.[41] In *Bancoult*, diplomatic cables from the US mission in London were sent to its home government, and to other non-specified third parties. Leaked documents were published on journals following an alleged illegitimate extraction by Wikileaks. Journal articles and diplomatic cables published were thus produced in court by private parties – who had no role in the taking of diplomatic cables.[42]

37 Schmitt (n. 3), 216.

38 Other than the already quoted literature, see Carlo Curti Gialdino, *Lineamenti di diritto diplomatico e consolare* (Torino: Giappichelli 2018, 33 ff. and 302 ff.; Naomi Burke, 'The Protection of Diplomatic Correspondence in the Digital Age: Time to Revise the Vienna Convention?' in: Paul Behrens (ed.), *Diplomatic Law in the New Millennium* (Oxford: Oxford University Press 2017), 204 ff.; Elena Carpanelli, 'On the Inviolability of Diplomatic Archives and Documents: The 1961 Vienna Convention on Diplomatic Relations to the Test of WikiLeaks', Riv. Dir. Int. 98 (2015), 834-851; and Karen Kaiser, 'Does the Inviolability of Archives Lead to a Catch-22 Situation?', Revista IUS 11 (2017), 183-200.

39 UKSC, *Bancoult No 3* (n. 5).

40 See also Tribunal Supremo (Spain), 9 May 2016, STS 1029/2016, ECLI:ES:TS:2016:1029, arguing that 'La mera información reflejada en un diario de gran tirada, que dice hacerse eco de los cables hechos públicos por Wikileaks, no puede ser tomada en consideración. No solo ignoramos la autenticidad de esa información, sino que la revelación de los cables procedentes de la Embajada americana no es sino una prueba obtenida de forma ilícita cuya consideración resulta vedada, de acuerdo con el artículo 11 de la LOPJ, conforme ha puesto de relieve en múltiples ocasiones el Tribunal Constitucional. El Tribunal ha reiterado que no se compadece con el derecho a la tutela judicial efectiva y con el derecho a un juicio justo (artículo 24 CE) el hecho de valerse de pruebas obtenidas mediante la vulneración de derechos fundamentales, secreto […] Por lo tanto, el motivo no puede prosperar'. See also ECJ (General Court), *Bank Mellat v. Council of the European Union,* judgment of 29 January 2013, case no. T-496/10, paras 98 ff.

41 UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 64.

42 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

 DOI 10.17104/0044-2348-2021-3-733

## 1. Relevant Provisions Under the VCDR

According to Art. 24 VCDR, 'The archives and documents of the mission shall be inviolable at any time and wherever they may be'.

Under Art. 27(2), 'The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions'.[43]

Whereas both Art. 24 and Art. 27(2) VCDR establish a duty upon the receiving State, none of them tackles the issue of use in court of unlawfully obtained evidence. In other words, it is not clearly regulated whether an unlawful conduct makes the evidence inadmissible in court (so called fruit of poisonous tree doctrine). The scope of application of the two provisions can of course overlap when the correspondence becomes part of the archives.[44] Both Arts 24 and 27(2) appear to have a quite extended scope of application as neither the correspondence nor the archives must bear external marks identifying them as 'diplomatic' post or archive (as opposed to Art. 27(3)(4) VCDR on courier bag).[45]

## 2. Host State's Obligations Under Arts 24 and 27(2) VCDR in *Bancoult*

The first issue dealt with by the British courts concerns the possibility for domestic courts to rely upon diplomatic documents extracted by a private party (not by the host State) who made them available online. The Court of Appeal,[46] relying upon Mann's arguments,[47] concluded that Arts 24 and 27(2)

43 The provision, contrary to Art. 24, does not specify that protection is afforded to correspondence 'wherever this may be'. Yet, due to the ancillary nature of correspondence to archives, part of the scholarship advocates for the extension of the protection also to correspondence where this does not reach the recipient for intrinsic problems in delivery (Denza (n. 12), 189); a circumstance, this last one, that encourages delivery by way of diplomatic courier (Stanisław E. Nahlik, 'Development of Diplomatic Law: Selected Problems', RdC 222 (1990), 187-346 (288) and Roberts (n. 13), 117). See also Carlo Curti Gialdino, 'Alcuni nuovi profili in tema di immunità diplomatiche', Ordine internazionale e diritti umani (2018), 428-434 (429), and Michael Richtsteig, *Wiener Übereinkommen über diplomatische und konsularische Beziehungen* (Baden-Baden: Nomos Verlag 2010), 55.

44 Denza (n. 12), 190.

45 VCDR, Art. 27(4): 'The packages constituting the diplomatic bag must bear visible external marks of their character and may contain only diplomatic documents or articles intended for official use.'

46 Bancoult, R (on the application of) v. Secretary of State for Foreign & Commonwealth Affairs, judgment of 23 May 2014, [2014] EWCA Civ 708. Supporting the line of reasoning, Carpanelli (n. 38), 839.

47 Frederick A. Mann, *Further Studies in International* Law (Oxford: Clarendon Press 1990), 327, and 337 ('"Inviolability", let it be stated once more, simply means freedom from official interferences. Official correspondence of the mission over the removal of which the receiving state has had no control can, as has been submitted above, be freely used in judicial proceedings.').

VCDR only protect the foreign State from an active intervention of the receiving State. Consequently, diplomatic cables can be used in court by private parties if the unlawful extraction is not attributed to the host State.[48] This is a formalistic interpretation that[49] admittedly appears functional to the protection of State sovereignty, as the VCDR would not limit the powers of domestic courts.

The Supreme Court did not agree with such a view.[50] According to the Supreme Court, the use in court of documents extracted by private parties would be inconsistent with the principle of support and protection of foreign diplomatic missions.[51] Hence, a solution again for the protection of sovereignty – this time of the State of origin of the mission.

48 EWCA, *Bancoult No 3* (n. 46), 708, para. 58 f. ('We see considerable force in the argument that was advanced by Mr Kentridge and rejected in Shearson Lehman. Inviolability involves the placing of a protective ring around the ambassador, the embassy and its archives and documents which neither the receiving state nor the courts of the receiving state may lawfully penetrate. If, however, a relevant document has found its way into the hands of a third party, even in consequence of a breach of inviolability, it is prima facie admissible in evidence. The concept of inviolability has no relevance where no attempt is being made to exercise compulsion against the embassy. Inviolability, like other diplomatic immunities, is a defence against an attempt to exercise state power and nothing more. In Shearson Lehman, the Court of Appeal was reluctant to hold that a document, originally obtained in violation of the archives of the ITC, should be admissible in a court of the receiving state. It felt that a court, as an arm of the receiving state, should play its part in protecting the archives of the ITC. But Mr Kentridge submitted that, in view of the existence of an adequate range of remedies available to the ITC if a relevant document was originally obtained in violation of its archives, there was no reason to give an extended meaning to the term "inviolable". This submission reflects the views expressed by Dr Mann in the publications to which we have already referred.').

49 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 18, quoting Jean Salmon, *Manuel de Droit Diplomatique* (Brussels: Bruylant 1994), 244.

50 Cf. Rosalyn Higgins, *Problems and Process: International Law and How We Use It* (Oxford: Clarendon Press 1995), 88; Nahlik (n. 43), 292, and Denza (n. 12), 167.

51 UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 71. See also International Tin Council (Intervener) (No 2) [1988] 1, WLR 16, *Shearson Lehman Bros Inc v. Maclaine, Watson and Co Ltd*; per Lord Bridge ('Mr Kentridge presented a forceful argument for the defendants based on the proposition that the only protection which the status of inviolability conferred by Article 24 of the Vienna Convention and Article 7(1) of the Order of 1972 affords is against executive or judicial action by the host state. Hence, it was submitted, even if a document was stolen, or otherwise obtained by improper means, from a diplomatic mission, inviolability could not be relied on to prevent the thief or other violator from putting it in evidence, but the mission would be driven to invoke some other ground of objection to its admissibility. I need not examine this argument at length. I reject it substantially for the reasons given by the Court of Appeal. The underlying purpose of the inviolability conferred is to protect the privacy of diplomatic communications. If that privacy is violated by a citizen, it would be wholly inimical to the underlying purpose that the judicial authorities of the host state should countenance the violation by permitting the violator, or anyone who receives the document from the violator, to make use of the document in judicial proceedings.').

 DOI 10.17104/0044-2348-2021-3-733

The solution adopted by the Supreme Court seems consistent with international case law suggesting that diplomatic archives must be protected – thus not only free from State seizures.[52]

Provided that Arts 24 and 27(2) VCDR are also applicable if the alleged unlawful conduct is not attributed to the receiving State, the Supreme Court dwells on the extent of the 'inviolability' therein provided for.

The Court specifies a number of circumstances in which 'inviolability' to correspondence and archives is not to be granted despite the applicability of the relevant rules of international law. In the first place, this privilege can be denied if this is necessary to ensure the survival of the host State itself.[53]

In the second place, 'inviolability' is denied if the relevant document was not part of the archives or of the official correspondence at the time of the extraction. Here the Supreme Court shifts its attention to the notions of 'archive' and 'correspondence' in order to determine their scope of application (thus the scope of the protection afforded).

The Supreme Court understands 'archives' broadly, so as to encompass means of electronic storage.[54] Nonetheless, it has refused to decide on whether the documents were part of diplomatic archives because the cable was sent to the US State Department *and* 'elsewhere'. With a 'procedural eye', the Court concluded that there was 'no indication from where the Wikileaks document emanate[d]'[55] at the time of the unlawful extraction. Furthermore, to argue that the document was not part of the archives of the US Embassy in London, the court stressed that 'once the document reached the State Department or any other addressee, it was, so far as appears and in the form in which it was there held, a document in the custody of the Federal Government of the United States of that other authority, and not part of the

52 I.C.J. Reports 1980, 36, Judgment, United States Diplomatic and Consular Staff in Tehran, para. 77 ('[…] the Iranian authorities are without doubt in continuing breach of the provisions of Articles 25, 26 and 27 of the 1961 Vienna Convention and of pertinent provisions of the 1963 Vienna Convention concerning facilities for the performance of functions, freedom of movement and communications for diplomatic and consular staff, as well as of Article 24 of the former Convention and Article 33 of the latter, which provide for the absolute inviolability of the archives and documents of diplomatic missions and consulates. This particular violation has been made manifest to the world by 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.').

53 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 17. See Quebec Court of King's Bench, Appeal Side, *Rose v. The King* [1947] 3 D.L.R. 618.

54 Vienna Convention on Consular Relations, Vienna, 24 April 1963, United Nations, Treaty Series, Vol. 596, 261, Art. 1(a)(k). See UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 11. In the scholarship, see Roberts (n. 13), 113.

55 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

London Embassy archive'.[56] No role plays, in the court's eye, the *intention* of the diplomatic mission not to make a document public nor the unlawfulness of the extraction[57] from the archives under the authority[58] of the mission. An effective 'control theory' approach that however seems inconsistent with the *ratio* of the VCDR, which has the aim to protect archives 'wherever they may be'.

After having excluded that the diplomatic cable was part of the US diplomatic archives in London at the time of the extraction, the Supreme Court also excluded the applicability of the inviolability granted to diplomatic correspondence. In the Court's eye, Art. 27(2) VCDR is only applicable for the communication between the mission and the Ministry of Foreign Affairs (or other diplomatic missions),[59] namely the US State Department. The provision is not applicable for communications with third parties or 'unprotected organ[s] of the government'.[60] For the Supreme Court, the sending of 'confidential' (rather than top secret) cables also to third parties excludes the applicability of Art. 27 VCDR,[61] unless it is proven that the extraction did take place *en route* from the mail destined to the Ministry of Foreign Affairs of the sending State.

Critiques to the positions of the Supreme Court have been expressed already within the bench. According to Lady Hale, the simple extraction of the document '[…] not […] from the mission, but from elsewhere in the United States',[62] does not necessarily mean that inviolability should be denied. The theory of control over documents should rather be integrated with a scrutiny of the will of the diplomatic mission to make the document available to subjects that are not the intended protected recipients of communication.[63]

56 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

57 See UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 71.

58 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20 ('There is no indication that the United States Embassy in London attached any reservation to or placed any limitation on the use or distribution of the cable by the State Department or any other authority to whom the cable went.').

59 See Roberts (n. 13), 115. See also *Questions relating to the Seizure and Detention of Certain Documents and Data* (Timor Leste v. Australia), Provisional Measures, Order of 3 March 2014, I. C. J. Reports 2014, 147.

60 UKSC, *Bancoult No 3* (n. 5), Lord Sumption: '[…] the Secretary of State is unable to establish that it was obtained by Wikileaks, and through them by The Guardian and The Telegraph, from the archives of the US embassy in London as opposed to some other unprotected organ of the US government. He has not therefore established the essential factual foundation for reliance on article 24 of the Vienna Convention.', para. 76.

61 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 20.

62 UKSC, *Bancoult No 3* (n. 5), Lady Hale, para. 125.

63 UKSC, *Bancoult No 3* (n. 5), Lady Hale, para. 126 f.

 DOI 10.17104/0044-2348-2021-3-733

## 3. 'Inviolability' Under the VCDR: Publicly Disseminated Cables and Open Issues

The third exception developed by the Supreme Court is strictly related to the internet-world, even though it is dealt with only out of caution, as the applicability of both relevant rules has already been excluded. This last exception appears to be a first in the case law.[64]

In the Court's eye, inviolability is not to be granted where the information at hand has become of public domain and is freely accessible.[65] Free access to information is incompatible with the need of confidentiality grounding the rules on inviolability – up to the point that the last one is ousted. However, the Court is silent on whether an unlawful extraction by the receiving State (which was not the case in the judgment) might have any consequences for private entities seeking to use in courts the documents extracted. A lack of transmission of procedural invalidity would help circumvent the protection afforded by the VCDR: States might commit an international wrongdoing by extracting diplomatic cables and making them available online to the general public, whilst private lawsuits may be decided based on such documents.

What appears relevant in the decision of the Supreme Court on this point is not the conclusion per se, but the methodological approach followed to advocate in favour of this additional exclusion to inviolability. The interpretation of the Court[66] is not founded on treaty-law, but on parallelisms with the domestic rules on confidential materials.[67] Although the solution does not necessarily seem inconsistent with the VCDR, as this could be interpreted to imply confidentiality as a necessary element of inviolability, the fact that it is grounded on domestic law seems to reduce the potential of the decision as a future international law leading case.

64 UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 74.

65 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 21, and UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 74 ('There is, however, a reservation of some importance which follows from the nature of the protection accorded by Article 24 of the Convention, as I have analysed it. It concerns documents which, although indirectly obtained without authority from the archives and documents of a mission, have entered the public domain. By that I mean that they have been disclosed not simply to a few people or in circumstances where it would take some significant effort on the part of others to discover their contents, but that they are freely available to anyone who cares to know.').

66 On which see Robert McCorquodale, 'Wikileaks Documents are Admissible in a Domestic Court', EJIL: Talk!, 21 February 2018.

67 UKSC, *Bancoult No 3* (n. 5), Lord Mance, para. 21. Generally referring to principles of confidentiality where secrecy has already been prejudiced, Lord Sumption, para. 74 ff.

DOI 10.17104/0044-2348-2021-3-733 ZaöRV 81 (2021)

What remains open is the burden of proof, unregulated in the VCDR. Some previous judgments have developed a presumption *iuris tantum* in whose light diplomatic documents should be presumed to be part of diplomatic archives or correspondence.[68] A solution that is certainly consistent with the VCDR framework. In *Bancoult 3*, only Lord Sumption, in a concurring opinion, stresses that the US State Department has not offered proof of the unlawful extraction from the diplomatic mission[69], thus failing to give proof of the 'essential factual foundation for reliance on article 24 of the Vienna Convention'.

All these critical elements, the transmission of procedural invalidity, the domestic interpretation of 'treaty relevant matters', and the question of the burden of proof, will have to be clearly determined in the future, possibly by States rather than courts – so as to ensure uniform application of the VCDR to online accessible reserved information.

## V. Online Crimes, and Diplomatic and Consular Privileges

The relationship between online (or cyber) crimes and diplomatic privileges should be analysed from different perspectives.[70]

The first scenario concerns the inviolability of the premises of the mission (rather than immunities of staff), either when these are subject to cyber attacks, or when the crime is committed from the Embassy or consular post itself. If the mission is the victim of online crimes, the receiving State should do as much as possible to 'prevent any disturbance of the peace of the mission or impairment of its dignity' (Art. 22(2) VCDR). Should the forces of the receiving State need to enter the premises to fulfil such obligation, two different regimes are applicable. For diplomatic premises, the VCDR sets an absolute inviolability, meaning that the public forces of the receiving State need pre-emptive authorisation to enter.[71] In Contrast for consular posts, inviolability is granted only to that part of the consular premises used exclusively for the purpose of the work of the consular post, and consent for

68 Quebec Court of King's Bench, *Rose* (n. 53), 646 ('International law creates a presumption of law that documents coming from an Embassy have a diplomatic character and that every Court of Justice must refuse to acknowledge jurisdiction or competence in regard to them.').

69 UKSC, *Bancoult No 3* (n. 5), Lord Sumption, para. 76.

70 On which, in general see Choi (n. 3), 120 ff.

71 VCDR, Art. 22(1). See Denza (n. 12), 118 f.; Wagner, Raasch and Pröbstl (n. 12), 182; d'Aspremont (n. 26), 5 f., Curti Gialdino (n. 19), 212.

 DOI 10.17104/0044-2348-2021-3-733

entrance is presumed in case of 'fire or other disaster requiring prompt protective action'.[72]

The scholarship has debated whether the 'disaster exception' can be extended from consular to diplomatic premises as well, or if there exists an implied presumed consent of the diplomatic mission where the action of the receiving State is necessary to save human lives.

Even if one should adhere to the (not unanimous) idea that also diplomatic premises are subject to an implied authorisation if an action is necessary to save human lives, it could scarcely be argued that cyber-attacks against the diplomatic mission amount to a threat of life.[73] In this sense, it appears that – at least as a general principle – authorisation from the head of the mission or the State of origin will be necessary.

As for consular posts, the question for those premises that do fall within the scope of application of inviolability is whether the term 'disaster' might also include cyber-crimes. Even though 'disasters' might not necessarily only be natural (as fires might also derive from the action of men), it should be stressed that such a provision is an exception to the general rule – hence it should be subject to a restrictive interpretation. Moreover, the *ratio* of the rule is to protect both the sovereignty of the foreign State, and the safety and security of the receiving State in whose territory a fire might expand from the consular post. In this sense, it appears that an unauthorised entrance into consular posts in cases of cyber-attacks could be deemed possible only to the extent such intervention is necessary to protect the host State itself, rather than only the post whose head does not grant access to.

The additional issue of eavesdropping or cyber-espionage may also be scrutinised through the lenses of the inviolability of the premises. If any device is 'implanted' in the mission for the purposes of cyber-espionage, this would amount to a violation of the inviolability of the premises. On the contrary, if information from the mission to the State of origin is 'intercepted' by other means, this could constitute a breach of the freedom of communication of the mission with its State enjoyed under Art. 27(1) VCDR.[74]

---

72 VCCR, Art. 31(2). See also Convention on special missions, New York, 8 December 1969, UNTS, Vol. 1400, 231, Art. 25(1) ('The premises where the special mission is established in accordance with the present Convention shall be inviolable. The agents of the receiving State may not enter the said premises, except with the consent of the head of the special mission or, if appropriate, of the head of the permanent diplomatic mission of the sending State accredited to the receiving State. Such consent may be assumed in case of fire or other disaster that seriously endangers public safety, and only in the event that it has not been possible to obtain the express consent of the head of the special mission or, where appropriate, of the head of the permanent mission.').

73 See Choi (n. 3), 123.

74 See in particular d'Aspremont (n. 26), 10 f., and Curti Gialdino (n. 38), 211.

The second scenario, on the other side, sees premises not as victims, but as the origin of cyber-attacks. The rules on inviolability remain the same; however, if the victim of the attack is the receiving State itself, this might advocate the necessity to overrule inviolability to ensure its own survival. If it is true that some courts have rejected inviolability of diplomatic communication to ensure self-preservation, the same should hold true also in the case of inviolability of premises.

Stronger, and potentially more difficult to be overruled, is the immunity from jurisdiction of diplomatic and consular staff where these are responsible for the cyber-attack against the receiving State. Personal and functional immunity of diplomatic agents is extended under Art. 31 VCDR, and the most common accepted reaction of the receiving State would generally be a declaration of *persona non grata*,[75] so as to rip immunities off after the expiration of the warning to leave the country.

The receiving State could have stronger reaction powers, namely the possibility to arrest and trial the responsible persons, if these are non-diplomatic staff at the Embassy and their acts are performed outside their duties (or, as a general rule, if they are nationals or habitual residents in the host State). A similar limitation to the possibility for the State to proceed to trial is given for consular staff members, whose immunity is also limited to official acts.[76]

## VI. Closing Remarks

The paper has examined four questions that have already emerged into practice, i. e. social media and diplomatic communications; digital embassies; online archives and diplomatic cables, and cyber-crimes involving diplomatic premises.

From the above case studies, it seems possible to identify scenarios that can be subsumed within the scope of application of 'traditional' rules of diplomatic law. Here, a certain flexibility and adaptability of the Vienna Conventions to the digital world emerges (despite the substantive adequacy of the solution). As the *Bancoult* judgment or the questions revolving around cyber-crimes involving diplomatic or consular premises suggest, many issues posed by the internet era to diplomatic law appear essentially to be hermeneutic in nature. Nonetheless, domestic jurisprudence also proves that interpretation and qualification matters are still open, as neither a significant and

75 Choi (n. 3), 121.
76 VCCR, Art. 43(1).

 DOI 10.17104/0044-2348-2021-3-733

consistent State practice subsequent to the Vienna Conventions, nor a specific interpretation of those treaties on 'internet-related issues', has been developed yet.

At the same time, the Vienna Conventions do not seem suited to other scenarios – such as the use of social media for official communication purposes by diplomats or Head of States, and the possibility to establish 'online posts'. Despite a reasonable flexibility in the interpretation of the rules of the Vienna Conventions, these appear unsuited to be applied to these new situations, leaving legal uncertainty as per their treatment under international law.

If legal certainty, as mentioned, is one of the preconditions for eDiplomacy to flourish, it seems that no clear prediction can be drawn in current times. Where for some delicate issues the codified rules of diplomatic law, one of the oldest fields of international law, appear inherently flexible enough to 'cope' with the most urgent challenges posed by the digital divide, the Vienna Conventions and international diplomatic law at large appear non-applicable in other circumstances.[77] As the basic approaches and the most fundamental legal assumptions of diplomatic law still rest upon a ritualistic conceptualisation of diplomatic functions and the treatment of diplomatic premises as 'sanctuaries', for the array of 'new challenges' States will need to develop 'new rules'. It seems however difficult to foresee if these new rules will be developed. This is because, on the one side, a specific legal framework would increase legal certainty and, to some extent, contribute in promoting eDiplomacy. At the same time, on the other side, such development might be to the detriment of traditional in person diplomacy.

77 Amongst the legal questions that have not been emerged with strength as case-studies, the existence of a 'right' of diplomatic or consular missions to access an adequate internet connection; international cooperation to ensure the establishment of proper internet-infrastructures in all States; privacy, secrecy, and data protection at large where eDiplomacy is carried out through third parties applications could be thought of.