7

Diplomatic and consular law

1. This Chapter sets out the international law governing diplomatic and consular relations applicable to State conduct in cyberspace. Diplomatic and consular law rests heavily on the 1961 Vienna Convention on Diplomatic Relations and the 1963 Vienna Convention on Consular Relations. The International Group of Experts agreed that these treaties substantially reflect customary international law.[481] Therefore, the Rules that follow significantly draw upon them.

2. The term 'receiving State' refers to the State to which a diplomatic mission or consular post is accredited. 'Sending State' is the State that the mission or post represents. It should be noted that a head of mission or other member of the diplomatic staff may be accredited to several States.[482] In such cases, the reference to 'receiving State' applies to all States to which the individual has been accredited.

3. As used in this Chapter, the term 'diplomatic mission' refers to a State's diplomatic presence in another State, established with the consent of the latter, for the purpose of representing the sending State in the receiving State and performing other functions set out in international law. 'Premises of a mission' refers to 'the buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used for the purposes of the mission'. The term includes the residence of the head of the mission.[483] A 'diplomatic agent' is the head of the mission or a member of the diplomatic staff of the mission.[484]

4. 'Consular post' denotes any consulate-general, consulate, vice-consulate, or consular agency of a sending State in a receiving State, established with the consent of the latter, for the purpose of performing

[481] *Tehran Hostages* judgment, paras. 62, 69.
[482] Vienna Convention on Diplomatic Relations, Art. 5.
[483] Vienna Convention on Diplomatic Relations, Art. 1(i).
[484] Vienna Convention on Diplomatic Relations, Art. 1(a), (d–e).

consular functions.[485] 'Consular premises' refers to the 'buildings or parts of buildings and the land ancillary thereto, irrespective of ownership, used exclusively for the purposes of the consular post'.[486] A 'consular officer' is 'any person, including the head of a consular post, entrusted in that capacity with the exercise of consular functions'.[487] A diplomatic mission may perform consular functions; no consent of the receiving State is required in these cases.[488] Although consular officers may in certain circumstances be authorised to perform diplomatic acts, doing so does not confer upon them any right to claim diplomatic privileges and immunities (Rule 44).[489]

5. The law that governs international organisations is not specifically addressed in this Chapter. However, major international organisations such as the United Nations and its specialised agencies enjoy immunities and privileges by treaty that are akin to those to which diplomatic missions are entitled. For example, they are entitled to inviolability of premises and communications, and representatives to these organisations benefit from privileges and immunities analogous to those afforded to diplomats or consular officers.[490] The law governing the privileges and immunities accorded to international organisations and their staff differs for each organisation and can be found in the constitutive treaties or other instruments that establish the organisations, as well as in agreements that the organisations conclude with their host States and other States where they need privileges or immunities for the performance of their functions.[491]

6. Similarly, the law governing special missions is not specifically dealt with in this Chapter. The 1969 Convention on Special Missions addresses the privileges and immunities that apply to 'special missions', that is, temporary missions representing a sending State in a receiving

[485] Vienna Convention on Consular Relations, Art. 1(1)(a).
[486] Vienna Convention on Consular Relations, Art. 1(1)(j).
[487] Vienna Convention on Consular Relations, Art. 1(1)(d).
[488] Vienna Convention on Diplomatic Relations, Art. 3(2); Vienna Convention on Consular Relations, Arts. 3, 70.
[489] Vienna Convention on Consular Relations, Art. 17.
[490] *See, e.g.*, UN Charter, Art. 105(1–2).
[491] *See, e.g.*, Convention on the Privileges and Immunities of the United Nations, 13 February 1946, 1 UNTS 15; Agreement Between the United Nations and the United States Regarding the Headquarters of the United Nations, 26 June 1947, 11 UNTS 147; Rome Statute, Art. 48; Headquarters Agreement between the International Criminal Court and the Host State, 7 June 2007, ICC-BD/04-01-08.

State with the consent of the latter for the purpose of dealing with it on specific questions or to perform a specific task.[492] Although the Convention has not been widely ratified and operates only with the consent of the receiving State, the International Group of Experts acknowledged support among States for the position that members of special missions enjoy immunity and inviolability as a matter of customary law, particularly in light of State practice affording special missions the privileges and immunities stipulated in the Convention. The Experts noted that when special missions make use of the facilities of their State's diplomatic missions, the inviolability of the premises and cyber infrastructure therein would protect their cyber activities as discussed in this Chapter irrespective of the applicability of the privileges and immunities to which special missions are entitled.

7. Many of the immunities set out in this Chapter apply to a more limited extent to family members of a diplomatic mission's or consular post's personnel, as well as to the administrative and technical staff of a mission or post and their families.[493] However, the commentary that follows does not address these immunities. The Vienna Convention on Diplomatic Relations, the Vienna Convention on Consular Relations, and the Convention on Special Missions set forth the specific scope of such immunities afforded to these individuals and should be consulted in this regard. With respect to the immunity of States and State officials under general international law, see Rule 12.

8. The International Group of Experts noted that the interrelationship of diplomatic and consular law with the rules of the law of State responsibility involving circumstances precluding wrongfulness (Rule 19) is especially complex. In particular, the Experts agreed that as set forth in Rule 22, countermeasures that would breach the inviolability (including the jurisdictional immunity) of diplomatic or consular agents (Rule 44), premises (Rule 39), or archives or documents (Rule 41) are prohibited.[494] Take the example of a sending State that is using the cyber infrastructure of a diplomatic mission to transmit espionage malware into computers in the receiving State. Doing so is an abuse of the diplomatic function[495] and therefore an internationally wrongful

[492] Convention on Special Missions, Art. 1, 8 December 1969, 1400 UNTS 23431.
[493] *See, e.g.,* Vienna Convention on Diplomatic Relations, Arts. 37–38; Vienna Convention on Consular Relations, Arts. 43.
[494] Articles on State Responsibility, Art. 50(2)(b) and paras. 14–15 of commentary.
[495] Vienna Convention on Diplomatic Relations, Art. 3(1).

act (Rule 14). Nevertheless, the receiving State is not allowed to engage in cyber operations directed at cyber infrastructure in the premises as a countermeasure.

9. The Experts agreed that pursuant to the principle of reciprocity, a receiving State may provide, with respect to a sending State's cyber-related activities, less favourable treatment to the sending State than it provides to other sending States when its mission or post is subjected to similar treatment in the sending State. They cautioned, nevertheless, that the receiving State may not act in a manner that violates diplomatic or consular law.[496] The Experts took note of the view, which none of them held, that a receiving State acting in violation of the provisions of diplomatic or consular law may be subject to a proportionate denial of reciprocal rights.

10. The International Group of Experts agreed that this Chapter generally applies during periods of armed conflict. In this regard, Article 45(a) of the Vienna Convention on Diplomatic Relations provides: 'The receiving State must, even in case of armed conflict, respect and protect the premises of the mission, together with its property and archives.' Article 27(1)(a) of the Vienna Convention on Consular Relations sets forth an equivalent protection for consular premises, property, and archives. Moreover, the two instruments state that the functions of a person enjoying diplomatic privileges and immunities subsist during a period of armed conflict until the person leaves the receiving State, or upon expiry of a reasonable period in which to do so.[497]

Rule 39 – Inviolability of premises in which cyber infrastructure is located

Cyber infrastructure on the premises of a diplomatic mission or consular post is protected by the inviolability of that mission or post.

1. Inviolability of the premises of a diplomatic mission is a bedrock principle of diplomatic law. By the principle, the premises may not be entered absent consent.[498] Additionally, property on the premises of a

[496] Vienna Convention on Diplomatic Relations, Art. 47(2); Vienna Convention on Consular Relations, Art. 72(2). *See also* Denza, Diplomatic Law, at 406–408.

[497] Vienna Convention on Diplomatic Relations, Art. 39(2); Vienna Convention on Consular Relations, Art. 53(3).

[498] Vienna Convention on Diplomatic Relations, Art. 22(1).

diplomatic mission is immune from search, requisition, attachment, or execution by the receiving State's agents without the sending State's consent.[499]

2. The International Group of Experts agreed that this Rule extends to the premises of a consular post, but the protection only encompasses those areas that are used exclusively for the purposes of the consular post.[500]

3. With respect to the application of this Rule, the International Group of Experts was divided over the lawfulness of remotely intruding into cyber infrastructure located in a sending State's diplomatic or consular premises, or otherwise disrupting or altering data therein. The majority of the Experts agreed that the Rule prohibits a receiving State from doing so on the basis that cyber operations manifesting on cyber infrastructure in the premises amount to unconsented-to entry into the premises. The Experts' conclusion is further supported by the receiving State's special duty to take all appropriate steps to protect the premises of a diplomatic mission against any intrusion or damage (Rule 40),[501] and its obligation to facilitate the full performance of the mission.[502]

4. A few of the Experts, however, were of the view that a violation of this Rule requires the receiving State's physical presence in the mission or post. For them, conducting a close-access cyber operation would, for example, satisfy this standard. They were also willing to characterise the remote causation of physical consequences in a diplomatic mission or consular post by cyber means as a violation of this Rule. To the extent the Rule protects the premises of diplomatic missions against non-consensual physical entry, the remote causation of physical consequences effectively amounts to physical presence therein for these Experts.

5. It must be cautioned that activities conducted remotely against a diplomatic mission's or consular post's cyber infrastructure or activities might violate other Rules set forth in this Chapter, such as that protecting diplomatic archives, documents, and official correspondence (Rule 41). In other words, the fact that a receiving State's cyber

[499] Vienna Convention on Diplomatic Relations, Art. 22(3).
[500] Vienna Convention on Consular Relations, Art. 31.
[501] Vienna Convention on Diplomatic Relations, Art. 22(2).
[502] Vienna Convention on Diplomatic Relations, Art. 25; Denza, Diplomatic Law, at 171–172.

operation does not violate this Rule does not necessarily render it lawful under diplomatic and consular law.

6. The International Group of Experts was divided as to whether a State other than the receiving State has an obligation to respect the inviolability of the premises of a diplomatic mission or consular post situated in the receiving State. Consider a case in which State A conducts a cyber operation to exfiltrate data from the cyber infrastructure in State B's embassy that is located in State C in order to determine the positions of State B's diplomatic personnel. The International Group of Experts was evenly split over this example. Some Experts took the position that State A has violated this Rule, noting that its behaviour is inconsistent with the object and purpose of the principle of inviolability, as well as the fact that remote access to cyber infrastructure is increasingly a mere technical matter. The other Experts adopted the contrary position on the ground that legal obligations in diplomatic law arise primarily from the relationship between sending and receiving States. They also pointed out that the specific obligations imposed on third parties in the relevant treaty texts are generally confined to the inviolability of official correspondence and communications that are in transit (Rule 41).[503]

7. The Experts concurred that a receiving State *in extremis* may take actions against the premises, or cyber infrastructure therein, of a diplomatic mission or consular post in self-defence (Rule 71).[504] For instance, if cyber infrastructure in a mission is being used to transmit critical information about the receiving State's armed forces for use in an imminent armed attack by the sending State, the receiving State may conduct operations, including at the use of force level, against that cyber infrastructure. The Experts acknowledged a view, which none of them held, by which the inviolability of the premises of a mission or post is absolute. Proponents of this view assert that the remedies available to a receiving State in such a scenario are those contained in diplomatic and consular law, such as the termination or suspension of diplomatic or consular relations, as well as the use of force in self-defence against targets other than the premises of the mission.

[503] Vienna Convention on Diplomatic Relations, Art. 40(1) and (3); Vienna Convention on Consular Relations, Art. 54(1) and (3).

[504] First report from the Foreign Affairs Committee, Session 1984–85: the abuse of diplomatic immunities and privileges, paras 88–95. *See also* Yearbook of the International Law Commission, Vol. II (1958), at 97; Denza, Diplomatic Law, at 223.

8. A separate question involves the protection of a diplomatic mission's property that is not on its premises, such as official mobile phones or laptops that are removed from the premises. The International Group of Experts was divided also on this question.

9. A majority of the Experts was of the view that such property enjoys inviolability under this Rule. Most of the Experts among the majority took the view that it is inviolable, as discussed above. Therefore, the sending State may not undertake cyber operations against it. For these Experts, extending inviolability to property that is located outside of the premises is in line with the object and purpose of the law governing diplomatic and consular inviolability. They noted that such property also is likely to qualify as inviolable 'archives' of a diplomatic mission under Rule 41, as there will usually be official diplomatic material stored on it. Finally, the Vienna Convention on Diplomatic Relations provides that the movable personal property of diplomatic agents is inviolable, subject only to exceptions for certain civil or administrative actions.[505] Therefore, for these Experts, it would be incongruent to conclude that property of a diplomatic mission is violable once removed from the premises, whereas the private property of a diplomatic agent enjoys inviolability, wherever located.

10. Some of the Experts among the majority concluded that such property is only immune from cyber operations that would constitute a search, requisition, attachment, or execution. They based their view on the fact that property on the diplomatic premises enjoys these forms of protection.[506] These Experts also observed that the Vienna Convention on Diplomatic Relations extends the same immunity to means of transport,[507] one of the principal forms of movable property at the time of its drafting. They further noted the emerging practice of recognising immunity from attachment of diplomatic bank accounts.[508]

11. A few of the Experts who were not in accord with the majority position opined that such property is not protected at all under this Rule,

[505] Vienna Convention on Diplomatic Relations, Art. 30(2); Yearbook of the International Law Commission, Vol. II (1958), at 98.

[506] Vienna Convention on Diplomatic Relations, Art. 22(3).

[507] Vienna Convention on Diplomatic Relations, Art. 22(3).

[508] *Alcom* v. *Republic of Colombia* AC 580 (12 April 1984) (UK); *Republic of 'A' Embassy Bank Account* Case, 77 ILR 489 (1986) (Austria); *MK* v. *State Secretary for Justice*, 94 ILR 357 (1988) (Neth.); *In the Matter of the Application of Liberian Eastern Timber Corp.* v. *The Government of Liberia*, 89 ILR 360 (1987) (US). *See also* the Convention on Jurisdictional Immunities, Art. 21; US Department of State Office of the Legal Advisor, Digest of United States Practice in International Law (2000), at 548.

citing the language in the Vienna Convention on Diplomatic Relations, which provides immunity from search, requisition, attachment, or execution only to the 'premises of the mission, their furnishings and other property thereon'.[509]

12. Given the complexity of the issue of property that is not on the premises of diplomatic missions, the Experts could come to no conclusion as to property removed from consular posts.

13. For a discussion of the placement of listening devices by the receiving State on the premises of a diplomatic mission, see Rule 41.

14. The International Group of Experts considered the announcements of a few States that they have established 'virtual embassies'. For example, the United States has launched websites that it describes as 'virtual embassies' in Iran and Syria, while Estonia has announced that it will establish a 'data embassy' in order to back up critical government data on servers located in friendly States. Given the contexts in which the United States and Estonia have invoked the terms 'virtual embassy' and 'data embassy', the Experts agreed that these entities, solely by virtue of the use of the term 'embassy', do not qualify as premises of a diplomatic mission. The Experts further pointed to the fact that mutual consent is required to establish diplomatic relations between States, and, in particular, to establish permanent diplomatic missions.[510] In the absence of such consent, a 'virtual embassy' is not entitled to special protection under diplomatic law. It should be noted that if the cyber infrastructure (such as computers, servers, or other network devices) upon which a so-called virtual or data embassy relies is located on the premises of a diplomatic mission, it falls under the protection set forth in this Rule. Furthermore, data relating to the 'virtual embassy' or 'data embassy' that also qualifies as official diplomatic correspondence or the archives or documents of the diplomatic mission (Rule 41) is protected as such.

15. The Experts likewise considered the 'online presences' of diplomatic missions. For example, it is now commonplace for diplomatic missions to create official accounts on social media platforms, such as Facebook. The International Group of Experts concluded that the inviolability of a diplomatic mission's premises does not apply to such a virtual presence. On the contrary, the premises of a diplomatic mission have been traditionally understood to imply physical presence.

[509] Vienna Convention on Diplomatic Relations, Art. 22(3).
[510] Vienna Convention on Diplomatic Relations, Art. 2.

Indeed, premises are defined in Article 1 of the Vienna Convention on Diplomatic Relations as 'buildings or parts of buildings and the land ancillary thereto'.[511] As with a 'virtual' or 'data embassy', however, the Experts acknowledged that if the online presence relies upon cyber infrastructure located in the physical premises of a diplomatic mission, said infrastructure falls within the scope of the protection established under this Rule. Moreover, the archives, documents, and official correspondence associated with the operation of the online presence may fall within the protective scope of Rules 41 and 42.

Rule 40 – Duty to protect cyber infrastructure

A receiving State must take all appropriate steps to protect cyber infrastructure on the premises of a sending State's diplomatic mission or consular post against intrusion or damage.

1. A receiving State has a 'special duty' to protect the premises of a diplomatic mission or consular post against intrusion or damage, irrespective of the source of the operation in question.[512] For instance, if the security services of the receiving State become aware that the sending State's cyber infrastructure within the premises of a diplomatic mission is being targeted by cyber operations, the receiving State must engage in all reasonable efforts to terminate the offending operations, including, where appropriate, notifying the sending State of the operations. Likewise, if the security services have information that the mission's cyber infrastructure is about to be targeted by cyber operations, the receiving State must take law enforcement or other measures that are proportionate and appropriate to the threat to prevent the operations.

2. The obligation set forth in this Rule is not absolute. The receiving State need only take 'all appropriate steps' to protect the premises.[513] As a general proposition, the extent of protection owed is based on, *inter alia*, the magnitude of the threat to the premises, the extent to which the

[511] *See also* Vienna Convention on Diplomatic Relations, Art. 21(1).

[512] Vienna Convention on Diplomatic Relations, Art. 22(2); *Tehran Hostages* judgment, paras. 61–66; Vienna Convention on Consular Relations, Art. 31(3). With respect to the premises of a diplomatic mission, *see also* Yearbook of the International Law Commission, Vol. II (1958), at 78, 95 (stating that a receiving State 'must, in order to fulfil this obligation, take special measures – over and above those it takes to discharge its general duty of ensuring order').

[513] Vienna Convention on Diplomatic Relations, Art. 22(2); Vienna Convention on Consular Relations, Art. 31(3).

receiving State is aware of a specific threat, and the capacity of the receiving State to take action in the circumstances. The receiving State enjoys the discretion to select the particular measures it will take to fulfil this duty.[514]

3. The International Group of Experts took notice of the fact that cyber operations targeting the premises of diplomatic missions or consular posts are often likely to originate from abroad, but could achieve no consensus as to whether a receiving State has a duty to seek assistance from those other States when necessary to protect premises on its territory. The majority was of the view that the receiving State bears no obligation to seek assistance under diplomatic and consular law; the duty to take 'appropriate steps' is limited to measures that involve the exercise of its sovereign authority. These Experts also took note of the apparent absence of State practice supporting the existence of such a duty. The minority was of the view that given the common benefit of maintaining diplomatic relations among States generally, it is reasonable to interpret this Rule as including a duty to seek assistance from other States when such assistance is likely to help put an end to the intrusive or damaging cyber operations.

4. The Experts agreed that there is no duty to take preventive measures to protect a diplomatic mission or consular post's premises and the cyber infrastructure therein until the receiving State is aware of a particular threat. In adopting this position, the Experts pointed to the common practice of receiving States in only providing special security personnel to protect the premises of a mission or post when there is a known security risk and, even then, only if requested by the head of a mission or post.[515] They further noted that, as a practical matter, the sending State is likely to rely on its own security measures to protect the cyber infrastructure on the premises of a mission or post, rather than those of the receiving State.

5. A receiving State is, however, obliged to take all appropriate steps to 'prevent any disturbance of the peace' of a diplomatic mission or consular post or the 'impairment of [their] dignity'.[516] Although this is an ill-defined

[514] *See, e.g., Ignatiev* v. *United States*, 238 F.3d 464 (D.C. Cir. 2001).

[515] *See, e.g.,* Australian Government, Department of Foreign Affairs and Trade, Protocol Guidelines, para. 12.2; Anthony Minnaar, *Protection of Foreign Missions in South Africa*, 9 *African Security Review* 67, 72 (2000).

[516] Vienna Convention on Diplomatic Relations, Art. 22(2); Vienna Convention on Consular Relations, Art. 31(3).

duty, the Experts agreed that the receiving State has no obligation to take steps against mere online expressions of criticism of a diplomatic mission or consular post or the sending State. Rather, the obligation is satisfied so long as the receiving State ensures that the actual functioning of the mission or post and the cyber infrastructure therein is not impaired. They observed that, in practice, States tend to balance the duty to prevent disturbance or impairment against the human rights of expression and assembly (Rule 35), and that although many States will impose certain restrictions on demonstrations in the immediate vicinity of embassies, they usually will refrain from prohibiting all speech in a particular medium that is critical of a sending State or its mission or post.[517]

6. This Rule should be read in conjunction with the other Rules set forth in this Chapter, especially that on the obligation to protect the free communication of a diplomatic mission or consular post (Rule 42), as well as applicable Rules set forth elsewhere in the Manual, such as those on due diligence (Rules 6–7).

Rule 41 – Inviolability of electronic archives, documents, and correspondence

Archives, documents, and official correspondence of a diplomatic mission or consular post that are in electronic form are inviolable.

1. International law affords broad inviolability to a diplomatic mission's or consular post's archives, documents, and official correspondence, including in electronic form.[518] The International Group of Experts agreed that 'inviolability' means that these materials are free from seizure, cyber espionage (see also Rule 32), enforcement, or judicial action, or any other form of interference by a State. The purpose of this protection is to ensure confidentiality.

2. Only States are bound by the Rule. It is not violated by the actions of private entities unless said actions are attributable to a State (Rules 15 and 17).

[517] *See, e.g., Finzer* v. *Barry*, 798 F.2d 1450 (D.C. Cir. 1986) (US); *Minister for Foreign Affairs and Trade and others* v. *Magno and another*, 112 ALR 529 (1992) (Austl.).

[518] Vienna Convention on Diplomatic Relations, Arts. 24, 27(2); Vienna Convention on Consular Relations, Arts. 33, 35(2). Note that the archives and documents of a consular post headed by an honorary consular officer shall be inviolable, but only if they are kept separate from other papers and documents. Vienna Convention on Consular Relations, Art. 61.

3. The International Group of Experts was of the view that 'archives', for the purposes of this Rule, include external hard drives, flash drives, and other media on which electronic documents are stored.[519] The term 'documents' includes not only final materials in electronic form, but also related drafts, negotiating documents, and other similar material that are amassed and deliberately preserved by diplomatic missions or consular posts in the course of their activities. 'Official correspondence' includes emails, demarches, cables, and other messages that relate to a diplomatic mission or consular post or the functions thereof.

4. The International Group of Experts was split over the issue of whether private submissions to a mission or post via email or through an online presence qualify as the archives, documents, or official correspondence protected by this Rule. For instance, the website of a diplomatic mission or consular post may allow nationals of the receiving State to submit online applications for visas to travel to the sending State. A majority of the Experts was of the view that the extension of inviolability in these circumstances is consistent with the object and purpose of diplomatic and consular law, and that once submitted for an official purpose, the information at least becomes part of the archives and documents of the mission or post. A few of the Experts took the contrary view that such private submissions are outside the scope of this Rule because diplomatic and consular law is limited to relations between States. However, all of the Experts agreed, for instance, that if a citizen of the receiving State posts a comment to the mission's most recent entry on a social media website, the comment is not protected by this Rule because it is publicly available.

5. In addition to the electronic archives, documents, and official correspondence of a diplomatic mission expressly cited in the Rule, inviolability encompasses the private papers and correspondence of diplomatic agents.[520] Inviolability does not, however, extend to the private papers and correspondence of consular officers or the staff of a consular post.[521]

[519] *See also* Vienna Convention on Consular Relations, Art. 1(1)(k) (defining 'consular archives' to include all the papers, documents, correspondence, books, films, tapes and registers of the consular post, together with the ciphers and codes, the card-indexes and any article of furniture intended for their protection or safe keeping).

[520] Vienna Convention on Diplomatic Relations, Art. 30(2).

[521] This conclusion is also supported by the fact that there is no comparable provision to Art. 30(2) of the Vienna Convention on Diplomatic Relations in the Vienna Convention on Consular Relations.

6. The inviolability of the archives and documents of a diplomatic mission or consular post attaches, in the view of the International Group of Experts, 'at any time and wherever they may be'.[522] Accordingly, electronic archives and documents of a mission or post are entitled to inviolability even when they are outside of the receiving State. To illustrate, if a diplomatic mission's archives are stored on a government server beyond the receiving State's territory, such as the sending State's Ministry of Foreign Affairs server, they remain inviolable. Similarly, if the material is stored on private cyber infrastructure, like a private email server or private cloud infrastructure, it remains protected so long as the sending State intends the material to remain confidential and it has not been disclosed to a third party with the consent (Rule 19) of the sending State.

7. The Experts agreed that treaty and customary law require all States – not just the receiving State – to accord official diplomatic and consular correspondence and other official communications 'in transit ... the same freedom and protection as the receiving State is bound to accord.'[523] Thus, they took the position that both the receiving and third States are prohibited from intercepting the electronic communications of diplomatic missions and consular posts that are in transit. In doing so, they noted that the confidentiality of diplomatic and consular communications is essential and central to the function of a diplomatic mission or consular post.

8. However, the Experts were divided over the question of whether all States, and not just the receiving State, are obliged to respect the inviolability of the sending State's diplomatic and consular material when that material is at rest as opposed to in transit. They noted that when the material is stored on the premises of a diplomatic mission or consular post, it may be protected by the premises' inviolability (see discussion in Rule 39). When that material is outside the mission or post, as in the case of data stored on a private cloud server, the Experts were divided. A minority of them took the view that extending the

[522] Vienna Convention on Diplomatic Relations, Art. 24; Vienna Convention on Consular Relations, Art. 33.

[523] Vienna Convention on Diplomatic Relations, Art. 40(3); Vienna Convention on Consular Relations, Art. 54(3). Third parties are also obliged to honour the inviolability of other categories of diplomatic and consular material in transit, such as the diplomatic or consular bag. Vienna Convention on Diplomatic Relations, Art. 40(3); Vienna Convention on Consular Relations, Art. 54(3). *See also, generally,* International Law Commission, Draft Articles on the Status of the Diplomatic Courier and the Diplomatic Bag Not Accompanied by Diplomatic Courier and Draft Optional Protocols (1989).

obligation to third States is consistent with the object and purpose of the principle of inviolability, particularly in light of the ease with which States can now access electronic data outside of their territory. The majority of the Experts adopted the contrary position on the ground that the specific obligations imposed on third parties in the relevant treaty texts are expressly confined to the inviolability of official correspondence and other communications in transit and thus do not extend to diplomatic or consular material that is at rest.

9. The Experts disagreed on the precise scope of the prohibition of electronic surveillance by third States of diplomatic communications. Specifically, they differed over whether the material that is protected from interception by a third State is confined to communications between a diplomatic mission and its sending government, or if it includes communications between the sending State and the receiving State, as well as between the mission of the sending State and the missions of other States in the receiving State.

10. A majority of the Experts was of the view that the prohibition extends to all such communications, citing the broad inviolability official correspondence enjoys in general; the fact that such communications come within the scope of 'all correspondence relating to the mission and its functions';[524] and the negotiating history of the Vienna Convention on Diplomatic Relations, which suggests that the principle of free communication (Rule 42) was not intended to be confined to communication between a diplomatic mission and its sending government, but rather was meant to extend to all official correspondence, including communication between the diplomatic mission of a sending State and the government of the receiving State or the diplomatic missions of other States.[525] In other words, the majority concluded that diplomatic law is, as a general matter, meant to foster the confidentiality of diplomatic communications and saw no reason to carve out an exception for this category. A few of the Experts took the position that the prohibition only encompasses the communications of a diplomatic mission with its sending government. They cited the absence of clear language prohibiting the interception of other types of communications and asserted that a fundamental object and purpose

[524] Vienna Convention on Diplomatic Relation, Arts. 27(1), 40(3) (suggesting the protection of official correspondence from interception by third parties, when taken together.).
[525] Yearbook of the International Law Commission Vol. II (1957), at 137–138.

of diplomatic law is to safeguard the ability of a mission to securely communicate with its own government.

11. The International Group of Experts noted that States appear to frequently have violated the aforementioned prohibitions, with numerous reports of surveillance by receiving States of the diplomatic communications of sending States and the placement of listening devices in the diplomatic missions of sending States. Even so, the Experts observed that in these instances sending States continue to object to surveillance as a violation of international law; condemnation of the practice usually goes unanswered, at least on the basis of international law, by States accused of such activities.[526] As a consequence, the Experts concluded that *opinio juris* has not formed in favour of regarding such surveillance as lawful. In other words, the extant international law prohibition of the surveillance of diplomatic material is undiminished.[527]

12. The materials encompassed by the Rule are protected on an indefinite basis. This is so even in the event of closure of the mission, severance of diplomatic relations, or armed conflict (Rules 82–83). Indeed, both the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations require the receiving State to 'respect and protect' the property and archives of a mission following breach of relations or recall of a mission's or post's personnel.[528]

13. The Experts were of the view that the inviolability of a diplomatic mission's or consular post's archives, documents, and official correspondence survives even if the material is stolen or obtained by a third party (including another State) using improper means and then provided, or otherwise made available, to a State obligated to respect its inviolability. Thus, States may not escape the obligation to respect the inviolability of diplomatic or consular material by employing or otherwise resorting to an intermediary who initially acquires the protected material. The Experts emphasised that the rules of attribution in the law of State responsibility (Rules 15–18) apply to this question.

[526] *See, e.g., China demands U.S. explain spying allegations linked to Australian missions*, Reuters, 31 October 2013; *Et Tu, UK? Anger Grows over British Spying in Berlin,* Spiegel Online, 5 November 2013; *MI5 Tried to Bug London Embassy, says Pakistan*, Kuwait News Agency, 6 November 2003.

[527] *See also Nicaragua* judgment, para. 186.

[528] Vienna Convention on Diplomatic Relations, Art. 45; Vienna Convention on Consular Relations, Art. 27(a).

14. On the question of whether inviolability survives if diplomatic or consular material is obtained by a third party (including another State) and then made available by the third party to members of the public, the International Group of Experts was divided. As an example, the material may be stolen or otherwise acquired improperly and posted on the Internet, as in the case of the Wikileaks incident. The majority took the position that this Rule no longer applies since its object and purpose of ensuring the confidentiality of the material has been defeated. In other words, if the material is openly accessible, it is not confidential as a matter of fact.[529]

15. A minority of the Experts was of the view that this Rule continues to apply in such cases. These Experts observed that continuing to respect inviolability insofar as is possible in the circumstances may assist in restoring the confidential nature of the material or preventing inferences being drawn from it that are adverse to the sending State or its diplomats. Furthermore, the sending State may wish to maintain the inviolability of the material with respect to States that have not yet accessed the information, while taking legal action against those within whose possession the material has come. Finally, these Experts pointed to the breadth of the norm of inviolability and its centrality to diplomatic relations, and thus interpreted the 'wherever they may be'[530] protective scope of documents as encompassing the public domain.

16. States are increasingly turning to an online presence to conduct certain diplomatic and consular functions, such as providing information about the receiving State's security situation for its citizens in the receiving State. In this regard, the International Group of Experts concluded that information or material made publicly available by the sending State is not entitled to the protection of this Rule because the object and purpose of the Rule is primarily to ensure the confidentiality of diplomatic and consular material. For instance, if one State defaces another State's diplomatic mission's website, this Rule is not implicated, although such action might violate a different Rule set forth in this Chapter, such as the inviolability of cyber infrastructure on diplomatic premises (Rule 39).

[529] *See, e.g., R (Bancoult)* v. *Secretary of State for Foreign and Commonwealth Affairs*, Court of Appeal Judgment [2014] EWCA Civ 708, para. 58 (finding a cable that had been leaked to the press containing diplomatic communications admissible in court).

[530] Vienna Convention on Diplomatic Relations, Art. 24; Vienna Convention on Consular Relations, Art. 33.

17. The International Group of Experts agreed that there is presently no requirement in customary international law for the electronic archives, documents, or official correspondence of a diplomatic mission or consular post to be marked as such for inviolability to attach. The Experts cited the absence of State practice to that effect and took note of the negotiating history of the Vienna Convention on Diplomatic Relations, during which proposals to impose such a condition on physical archives were rejected.[531]

18. The International Group of Experts noted the increasing use of honorary consular officers. In an effort to encourage economic ties while reducing the costs of establishing consular posts, many States employ businessmen and -women or other professionals to act as consular representatives on a part-time basis. Although the documents, correspondence, and archives of a consular post headed by an honorary consular officer are inviolable, this protection is conditional on the materials being kept separate from materials relating to the honorary consular officer's other professional activities.[532]

Rule 42 – Free communication

A receiving State must permit and protect the free cyber communication of a diplomatic mission or consular post for all official purposes.

1. International law provides that a receiving State must permit and protect the 'free communication' on the part of a sending State's diplomatic mission or consular post for all official purposes.[533] The International Group of Experts agreed that this provision reflects customary international law.

2. With respect to consular posts, of particular note is the right of consular officers to communicate freely with the sending State's nationals.[534] Therefore, the receiving State may not, for instance, interfere with

[531] United Nations Conference on Diplomatic Intercourse and Immunities, *United States of America: amendment to article 22*, A/CONF.20/C.1/L.153 (14 March 1961); United Nations Conference on Diplomatic Intercourse and Immunities, Official Records, A/CONF.20/14, at 149 (21 March 1961).

[532] Vienna Convention on Consular Relations, Art. 61.

[533] Vienna Convention on Diplomatic Relations, Art. 27(1); Vienna Convention on Consular Relations, Art. 35(1).

[534] Vienna Convention on Consular Relations, Art. 36(1)(a).

email communications between consular officers and the sending State's nationals regarding official consular matters.

3. The Experts noted that the Vienna Convention on Consular Relations uses the term 'permit and protect freedom of communication' in lieu of 'freedom communication', which more clearly conveys the object and purpose of the provision. For the Experts, the term 'permit' and the reference to 'freedom' mean that receiving States may not impede the capability of a diplomatic mission or consular post to communicate through cyber or other electronic means. For instance, they may not interfere with access to a diplomatic mission's or consular post's website that is used to convey essential information to its citizens in the country, interrupt or slow the Internet connection of a diplomatic mission or consular post, or block or interfere with its cell phones or other telecommunications equipment. The term 'permit' is not meant to imply that the sending State must seek the approval of the receiving State to engage in cyber communication.

4. The obligations of a receiving State go beyond permitting the free cyber communication of a diplomatic mission or consular post. The receiving State must also take action to 'protect' their communications from interruption by others. The International Group of Experts was of the view that the same standard that applies to the duty to protect cyber infrastructure on the premises of a mission or post (Rule 40) extends to the protection of free cyber communication; a receiving State must take 'all appropriate steps' to ensure said protection. As with the protection of the cyber infrastructure, this is not an absolute duty. The specific obligation is proportionate to the risk and the dangers threatening the cyber communications.

5. On the basis of the duty to protect, the Experts concurred that, for instance, should the authorities of the receiving State learn, from the sending State or any other source, that the sending State's cyber communications are being impeded, it must take appropriate steps to terminate the impediment. They also agreed that the receiving State is likewise obligated to take such measures to stop the interception of diplomatic cyber communications, including by other States (Rule 41), occurring on its territory.[535]

[535] Cyber communications present special challenges with regard to the obligation to protect. Consider the 2002 case in which unknown persons intercepted politically sensitive emails sent by the European Union's ambassador to Turkey, which were then shared with and published by a Turkish magazine. The Turkish government promised to investigate the incident and prosecute those involved, and after several days banned further publication of the emails, but it also observed that Internet surveillance is a widespread problem for which no State has been able to develop an effective response.

6. The Experts emphasised that the obligations of a receiving State to 'permit' and 'protect' are limited to cyber communications that are 'official'. For instance, if hackers in the receiving State are targeting a mission's or a post's official website, the receiving State must take those measures that are reasonably available to terminate the activity. Yet, a receiving State would not be obliged to permit and protect the capacity of diplomatic agents to engage in personal communications, for instance, through personal email accounts. The Experts acknowledged that it is sometimes difficult to distinguish between official and unofficial functions. This is particularly the case with regard to public diplomacy, which is directed at the receiving State's population. In the absence of *opinio juris* in this area, the Experts were unable to come to a definitive conclusion on this matter.

7. The International Group of Experts considered whether a receiving State is in violation of this Rule when it prohibits a diplomatic mission from establishing and operating an online presence, such as a website or social media account, on the basis that official business with the receiving State is required to be conducted with or through the Ministry for Foreign Affairs, or such other ministry as may be agreed, as set forth in Article 41(2) of the Vienna Convention on Diplomatic Relations. The Experts agreed that the requirement in Article 41(2) is only meant to clarify who within the receiving State's government should be the primary formal point of contact for official business between the sending and the receiving State. The Experts noted that many official business activities undertaken by foreign diplomatic agents in receiving States occur outside of these official channels; that it is customary for ambassadors and other diplomatic agents to give speeches to private audiences, hold roundtables, and otherwise interact on an official basis with private parties in the receiving State; and that these are accepted methods of exercising the diplomatic functions of representing the sending State, ascertaining conditions and developments in the receiving State, and promoting friendly relations between sending and receiving States.

Rule 43 – Use of premises and activities of officials

(a) The premises of a diplomatic mission or consular post may not be used to engage in cyber activities that are incompatible with diplomatic or consular functions.

(b) Diplomatic agents and consular officials may not engage in cyber activities that interfere in the internal affairs of the receiving State or are incompatible with the laws and regulations of that State.

1. The premises of a diplomatic mission may not be used in any manner incompatible with the functions of a diplomatic mission.[536] Such functions include, but are not limited to:

(a) Representing the sending State in the receiving State;
(b) Protecting the interests of the sending State and of its nationals in the receiving State, within the limits permitted by international law;
(c) Negotiating with the Government of the receiving State;
(d) Ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State; and
(e) Promoting friendly relations between the sending State and the receiving State, and developing economic, cultural, and scientific relations.[537]

2. Similarly, consular posts may not be used in any manner incompatible with consular functions.[538] Consular functions of relevance to cyber activities include, but are not limited to:

(a) Protecting in the receiving State the interests of the sending State and of its nationals (both individuals and legal persons), within the limits permitted by international law;
(b) Furthering the development of commercial, economic, cultural, and scientific relations between the sending State and the receiving State;
(c) Ascertaining conditions and developments in the commercial, economic, cultural, and scientific life of the receiving State and reporting thereon to the sending State, as well as providing such information to interested persons;
(d) Issuing passports and travel documents to nationals of the sending State, and visas or appropriate documents to persons wishing to travel to the sending State;
(e) Assisting nationals, both individuals and bodies corporate, of the sending State; and

[536] Vienna Convention on Diplomatic Relations, Art. 41(3).
[537] Vienna Convention on Diplomatic Relations, Art. 3.
[538] Vienna Convention on Consular Relations, Art. 55(2).

(f) Transmitting judicial and extrajudicial documents or executing letters rogatory or commissions to take evidence for the courts of the sending State.[539]

3. For instance, a sending State may not use the premises of its diplomatic mission to engage in cyber espionage against the receiving State (see also discussion in Rule 41). Using a diplomatic mission's cyber infrastructure to engage in commercial activity, such as e-commerce, would likewise fail to qualify as a diplomatic function.

4. A separate issue is whether it is permissible for a sending State to use the premises of its diplomatic mission or consular post, without the consent of the receiving State, as a base to engage in cyber espionage directed at a third State, whether that espionage occurs against the third State's organs located in the receiving State or beyond it. A majority of the International Group of Experts concluded that such practices are prohibited by *lit.* (a) of this Rule since they are inconsistent with accepted diplomatic functions. A few of the Experts countered that diplomatic relations are bilateral in character and do not bring about obligations *vis-à-vis* third States. Furthermore, they suggested that insufficient State practice and expressions of *opinio juris* exist to conclude that such a prohibition has crystallised into customary international law. They pointed in particular to long-standing allegations of State practice to the contrary.

5. Reflected in *lit.* (b) is the fact that it is the duty of diplomatic agents and consular officers 'to respect the laws and regulations of the receiving State'.[540] For example, in most instances it would be a violation of *lit.* (b) for a diplomatic agent to engage in online piracy of intellectual property while in the receiving State because such activities are likely to violate the receiving State's laws and regulations.

6. Pursuant to *lit.* (b), diplomatic agents and consular officials are also prohibited from interfering in the internal affairs of the receiving State.[541] For instance, diplomatic agents may not use social media to plot the removal of the receiving State's government or participate 'in political campaigns'. On the other hand, they may engage in cyber activities 'for the purpose of protecting the interests of the diplomatic agent's country or of its nationals in accordance with international

[539] Vienna Convention on Consular Relations, Art. 5.
[540] Vienna Convention on Diplomatic Relations, Art. 41(1); Vienna Convention on Consular Relations, Art. 55(1).
[541] Vienna Convention on Diplomatic Relations, Art. 41(1); Vienna Convention on Consular Relations, Art. 55(1).

law'.[542] As an illustration, the Experts agreed that they may use social media to urge the release of their citizens from detention by the receiving State on the grounds that the detention is unlawful or otherwise inappropriate; they acknowledged a view that doing so constitutes interference in internal affairs, but disagreed with it.

7. Due to their immunity from the receiving State's criminal, civil, and administrative process (Rule 44), diplomatic agents may not be subjected to enforcement or judicial jurisdiction (Rules 8–9) for engaging in activities that violate this Rule. They may be declared *persona non grata*, which would require the sending State to withdraw them.

8. Both the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations provide that a diplomatic mission and a consular post, respectively, may install and use a 'wireless transmitter' only with the consent of the receiving State.[543] At the time of the drafting of the Conventions, wireless transmitters were primarily used for radio transmissions. The International Group of Experts opined that this treaty language is to an extent dated and its precise translation to cyber technologies is not entirely clear. In particular, the Experts took the view that equipment that generally emits radio frequency signals only within the perimeter of a diplomatic mission or consular post, such as a wireless router, falls outside of the rule. But the Experts did agree that as new forms of wireless technology emerge, this principle should continue to require the receiving State's consent for the installation and use of equipment that allows the diplomatic mission or consular post to transmit communications beyond its premises. This would include the installation of all types of wireless communication equipment (e.g., for satellite communications) when their use is capable of causing harmful interference with wireless communications in the receiving State (on harmful interference, see also Rule 63).

Rule 44 – Privileges and immunities of diplomatic agents and consular officers

To the extent diplomatic agents and consular officers enjoy immunities from criminal, civil, and administrative jurisdiction, they enjoy the immunities with regard to their cyber activities.

[542] Yearbook of the International Law Commission, Vol. II (1958), at 104.
[543] Vienna Convention on Diplomatic Relations, Art.27(1); Vienna Convention on Consular Relations, Art. 35(1).

1. This Rule sets forth the immunities enjoyed by diplomatic agents and consular officers. Such immunities may always be waived by the sending State.[544]

2. Diplomatic agents are entitled to immunity from the criminal jurisdiction of the receiving State for any activity that qualifies as cyber crime under the receiving State's domestic laws while present in the country.[545] This diplomatic immunity is absolute and unqualified. They also enjoy immunity from arrest and are exempt from the obligation to give evidence as a witness.[546] Following completion of their diplomatic functions and departure from the receiving State, the privileges and immunities normally cease, although immunity for acts performed in the exercise of official functions continues (Rule 12).[547]

3. Diplomatic agents also enjoy immunity from the receiving State's civil and administrative jurisdiction with respect to their cyber activities, except in the case of certain actions relating to 'private immovable' (or 'real') property, succession, and any of the diplomatic agent's professional or commercial activities that were engaged in while in the receiving State and outside his or her official functions.[548] For example, a diplomatic agent might not enjoy immunity from civil or administrative jurisdiction for selling goods online as a personal business.

4. Consular officers are entitled to more limited immunity from the criminal and civil jurisdiction of the receiving State for their cyber activities.[549] In particular, they do not enjoy absolute immunity from the receiving State's criminal jurisdiction; however, they are not liable to arrest or detention pending trial, except in the case of a grave crime, and pursuant to a decision by a competent judicial authority.[550]

[544] Vienna Convention on Diplomatic Relations, Art. 32(1); Vienna Convention on Consular Relations, Art. 45(1).

[545] Vienna Convention on Diplomatic Relations, Art. 31(1). Members of the family of a diplomatic agent, administrative, and technical staff, and others associated with the mission are entitled to specific privileges and immunities. Vienna Convention on Diplomatic Relations, Art. 37.

[546] Vienna Convention on Diplomatic Relations, Arts. 29, 31(2).

[547] Vienna Convention on Diplomatic Relations, Art. 39(2).

[548] Vienna Convention on Diplomatic Relations, Art. 31(1).

[549] *Compare* Vienna Convention on Diplomatic Relations, Art. 29, *with* Vienna Convention on Consular Relations, Arts. 41, 43–44.

[550] Vienna Convention on Consular Relations, Art. 41. Note that honorary consular officers do not enjoy immunity from criminal proceedings. Vienna Convention on Consular Relations, Art. 63.