1

States and cyberspace

1. The purpose of this chapter is to set forth rules of a general international legal nature detailing the relationship between States, cyber infrastructure, and cyber operations. Section 1 addresses issues relating to State sovereignty, jurisdiction, and control over cyber infrastructure. Section 2 deals with the application of classic public international law rules of State responsibility to cyber operations.

2. Terminology is essential to an accurate understanding of this chapter. 'Cyber infrastructure' refers to the communications, storage, and computing resources upon which information systems operate (Glossary). To the extent States can exercise control over cyber infrastructure, they shoulder certain rights and obligations as a matter of international law. The term 'cyber operations' refers to the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace (Glossary). Under international law, States may be responsible for cyber operations that their organs conduct or that are otherwise attributable to them by virtue of the law of State responsibility. The actions of non-State actors may also sometimes be attributed to States.

3. Except when explicitly noted otherwise, the Rules and Commentary of this chapter apply both in times of peace and in times of armed conflict (whether international or non-international in nature). During an international armed conflict, the law of neutrality also governs the rights and obligations of States with regard to cyber infrastructure and operations (Chapter 7).

SECTION 1: SOVEREIGNTY, JURISDICTION, AND CONTROL

Rule 1 – Sovereignty

A State may exercise control over cyber infrastructure and activities within its sovereign territory.

1. This Rule emphasizes the fact that although no State may claim sovereignty over cyberspace *per se*, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure.

2. The accepted definition of 'sovereignty' was set forth in the *Island of Palmas* Arbitral Award of 1928. It provides that 'Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.'[1]

3. It is the sovereignty that a State enjoys over territory that gives it the right to control cyber infrastructure and cyber activities within its territory. Accordingly, cyber infrastructure situated in the land territory, internal waters, territorial sea (including its bed and subsoil), archipelagic waters, or national airspace is subject to the sovereignty of the territorial State.[2]

4. Sovereignty implies that a State may control access to its territory and generally enjoys, within the limits set by treaty and customary international law, the exclusive right to exercise jurisdiction and authority on its territory. Exceptions include the use of force pursuant to the right of self-defence (Rule 13) and in accordance with actions authorized or mandated by the United Nations Security Council (Rule 18).

5. A State's sovereignty over cyber infrastructure within its territory has two consequences. First, that cyber infrastructure is subject to legal and regulatory control by the State.[3] Second, the State's territorial sovereignty protects such cyber infrastructure. It does not matter whether it belongs to the government or to private entities or individuals, nor do the purposes it serves matter.

6. A cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage. The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage (as with malware used to monitor activities) constitutes a violation of sovereignty.

[1] *Island of Palmas* (*Neth.* v. *US*) 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

[2] On sovereignty over waters and airspace above waters, see Law of the Sea Convention, Art. 2; on sovereignty over airspace, see Chicago Convention, Arts. 1–3. With regard to cyber infrastructure in outer space, see Rules 3 and 4 and accompanying Commentary.

[3] In the 1949 *Corfu Channel* case, Judge Alejandro Alvarez appended a separate opinion in which he stated: 'By sovereignty, we understand the whole body of rights and attributes which a State possesses in its territory, to the exclusion of all other States, and also in its relations with other States. Sovereignty confers rights upon States and imposes obligations upon them.' *Corfu Channel* case at 43 (individual opinion of Judge Alvarez).

7. If such cyber operations are intended to coerce the government (and are not otherwise permitted under international law), the operation may constitute a prohibited 'intervention'[4] or a prohibited 'use of force' (Rules 10 to 12). A cyber operation that qualifies as an 'armed attack' triggers the right of individual or collective self-defence (Rule 13). Actions not constituting an armed attack but that are nevertheless in violation of international law may entitle the target State to resort to countermeasures (Rule 9). Security Council-mandated or authorized actions under Chapter VII of the United Nations Charter (Rule 18), including those involving cyber operations, do not constitute a violation of the target State's sovereignty.

8. A State may consent to cyber operations conducted from its territory or to remote cyber operations involving cyber infrastructure that is located on its territory. Consider a case in which non-State actors are engaged in unlawful cyber activities on State A's territory. State A does not have the technical ability to put an end to those activities and therefore requests the assistance of State B. State B's ensuing cyber operations on State A's territory would not be a violation of the latter's sovereignty. Consent may also be set forth in a standing treaty. For example, a basing agreement may authorize a sending State's military forces to conduct cyber operations from or within the receiving State's territory.

9. Customary or treaty law may restrict the exercise of sovereign rights by the territorial State. For example, international law imposes restrictions on interference with the activities of diplomatic premises and personnel. Similarly, a State's sovereignty in the territorial sea, archipelagic waters or straits used for international navigation is limited under customary international law by the rights of innocent passage, archipelagic sea lanes passage, and transit passage, respectively.[5]

10. In the cyber context, the principle of sovereignty allows a State to, inter alia, restrict or protect (in part or in whole) access to the Internet, without prejudice to applicable international law, such as human rights or international telecommunications law.[6] The fact that cyber infrastructure located in a given State's territory is linked to the global telecommunications network cannot be interpreted as a waiver of its sovereign rights over that infrastructure.

11. A coastal State's sovereignty over the seabed lying beneath its territorial sea allows that State full control over the placement of any submarine cables thereon. This is a critical right in light of the fact that

[4] UN Charter, Art. 2(1). [5] Law of the Sea Convention, Arts. 17–19, 37–8, 52, 53.
[6] *E.g.*, the ITU Constitution.

submarine cables currently carry the bulk of international Internet communications. As to submarine cables beyond the territorial sea, Article 79(2) of the Convention on the Law of the Sea limits the extent to which a coastal State may interfere with submarine cables on its continental shelf.[7]

12. Although States may not exercise sovereignty over cyberspace *per se*, States may exercise their jurisdiction *vis-à-vis* cyber crimes and other cyber activities pursuant to the bases of jurisdiction recognized in international law (Rule 2).[8]

13. With regard to cyber infrastructure aboard sovereign immune platforms, see Rule 4.

14. Traditionally, the notion of the violation of sovereignty was limited to actions undertaken by, or attributable to, States. However, there is an embryonic view proffered by some scholars that cyber operations conducted by non-State actors may also violate a State's sovereignty (in particular the aspect of territorial integrity).

Rule 2 – Jurisdiction

Without prejudice to applicable international obligations, a State may exercise its jurisdiction:

(a) over persons engaged in cyber activities on its territory;
(b) over cyber infrastructure located on its territory; and
(c) extraterritorially, in accordance with international law.

1. The term 'jurisdiction' encompasses the authority to prescribe, enforce, and adjudicate. It extends to all matters, including those that are civil, criminal, or administrative in nature. The various general bases of jurisdiction are discussed below.

2. The principal basis for a State to exercise its jurisdiction is physical or legal presence of a person (*in personam*) or object (*in rem*) on its territory. For instance, pursuant to its *in personam* jurisdiction a State may adopt laws and regulations governing the cyber activities of individuals on its territory. It may also regulate the activities of privately owned entities registered (or otherwise based as a matter of law) in its jurisdiction but physically operating abroad, such as Internet service providers ('ISPs'). *In rem* jurisdiction would allow it to adopt laws governing the operation of cyber infrastructure on its territory.

[7] Law of the Sea Convention, Art. 79(2).
[8] *See, e.g.*, Council of Europe, Convention on Cybercrime, 23 November 2001, Eur. T.S. No. 185.