INTERNATIONAL LAW STUDIES
PUBLISHED SINCE 1895
U.S. NAVAL WAR COLLEGE

Territorial Sovereignty and Neutrality in Cyberspace

Wolff Heintschel von Heinegg

89 INT'L L. STUD. 123 (2013)

Volume 89 2013

Territorial Sovereignty and Neutrality in Cyberspace

Wolff Heintschel von Heinegg[*]

I. INTRODUCTION

Because of its mystifying characteristics, cyberspace has been called a "fifth dimension" or a "fifth domain." There seems to be a widespread belief that it eludes the traditional rules and principles of international law, and that there is an urgent need for new rules specifically designed for cyberspace. All too often in the past we witnessed a considerable degree of perplexity vis-à-vis new technologies that resulted in similar desperate calls for new norms; however, only in rare cases were such calls justified. If analyzed soberly, international law as it currently exists need not capitulate to the novelty of the technology on which cyberspace is based or to the threats that did not exist prior to the cyber age. Interestingly, States seem to agree that customary international law is, in principle, applicable to cyber-

* Stockton Professor, U.S. Naval War College; Professor of Public Law, Europa-Universität Viadrina, Frankfurt (Oder), Germany. This article is a modified version of *Legal Implications of Territorial Sovereignty in Cyberspace* and *Neutrality in Cyberspace*, both articles published in 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT PROCEEDINGS 2012, at 1, 27 (Christian Czosseck, Rain Ottis & Kathartina Ziolkowski eds., 2012). The views expressed in this article are the sole responsibility of the author and do not reflect the view of the author's affiliations.

space, although there may be a need for a consensual adaptation to the specific characteristics of cyberspace.

This article will explore whether—and to what extent—the principle of territorial sovereignty and the law of neutrality apply to cyberspace. It will be shown that certain components of—and certain activities in—cyberspace are governed by the principle of territorial sovereignty and that neither general international law nor the law of neutrality has become obsolete merely because cyberspace may be considered a fifth dimension or part of the global commons.

II. TERRITORIAL SOVEREIGNTY

A. General Characteristics of Territorial Sovereignty

Under the principle of territorial sovereignty a State exercises full and exclusive authority over its territory.[1] As stated by Judge Max Huber in the *Palmas Island* arbitration award, "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 exclusivity of any other States, the functions of a State."[2] The International Court of Justice (ICJ) has emphasized that "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[3] Territorial sovereignty, therefore, implies that, subject to applicable customary or conventional rules of international law, the State alone is entitled to exercise jurisdiction, especially by subjecting objects and persons within its territory to domestic legislation and to enforce these rules. Moreover, the State is entitled to control access to and egress from its territory. The latter right seems to also apply to all forms of communication. Finally, territorial sovereignty protects a State against any form of interference by other States. While such interference may amount to a use of force, this article does not address that issue.

It must be remembered that territorial sovereignty is relative in character insofar as it does not merely afford protection to States, but also imposes obligations on States, especially the "obligation to protect within the ter-

1. *See, e.g.*, S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18–20 (Sept. 7) [hereinafter *Lotus*]; Free Zones of Upper Savoy and Gex (Fr. v. Switz.), 1932 P.C.I.J. (ser. A/B) No. 46, at 166–68 (June 7).

2. Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

3. Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 6, 35 (Apr. 9) [hereinafter *Corfu Channel*].

ritory the rights of other States, in particular their right to integrity and inviolability in peace and in war, together with the rights which each State may claim for its nationals in foreign territory."[4]

B. Territorial Sovereignty and Cyberspace

"Cyberspace" has been defined as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[5] There is a widely held view that it "is not a physical place—it defies measurement in any physical dimension or time space continuum. It is a shorthand term that refers to the environment created by the confluence of cooperative networks of computers, information systems, and telecommunication infrastructures commonly referred to as the World Wide Web."[6] It is true that cyberspace is characterized by anonymity and ubiquity.[7] It seems logical, therefore, to assimilate it to the high seas, international airspace or outer space,[8] that is, to consider it a "global common" or, legally, a *res communis omnium*.[9] However, these characterizations merely lead to the obvious

4. Island of Palmas, *supra* note 2, at 839. In his separate opinion in the *Corfu Channel* case, Judge Alvarez 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*, *supra* note 3, at 43.

5. Joint Chiefs of Staff, Joint Publication 1-02, DOD Dictionary of Military and Associated Terms (Nov. 8, 2010), as amended through July 15, 2012, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf [hereinafter Dictionary of Military and Associated Terms]. See also the definition by Arie J. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, 64 AIR FORCE LAW REVIEW 121, 126 (2009) (a "domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures").

6. THOMAS C. WINGFIELD, THE LAW OF INFORMATION CONFLICT: NATIONAL SECURITY LAW IN CYBERSPACE 17 (2000).

7. It has been rightly stated that "global digital networks have the features they do—of placelessness, anonymity, and ubiquity—because of politics, not in spite of them." *See* Geoffrey L. Herrera, Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space 12 (2006) (paper prepared for the 47th Annual International Studies Association Convention March 22–25, 2006), http://www.allacademic.com/meta/p98069_index.html.

8. For an analysis to that effect, see Patrick W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, 64 AIR FORCE LAW REVIEW 1, 17–42 (2009).

9. U.S. Department of Defense, Department of Defense Strategy for Operating in Cyberspace (2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf [here-

conclusion that cyberspace in its entirety is not subject to the sovereignty of a single State or group of States—that it is immune from appropriation.

Despite the correct classification of "cyberspace as such" as a *res communis omnium*, State practice provides sufficient evidence that components of cyberspace are not immune from territorial sovereignty nor from the exercise of State jurisdiction. States have exercised, and will continue to exercise, their criminal jurisdiction over cyber crimes[10] and they continue to regulate activities in cyberspace. Moreover, the simple truth that "cyberspace requires a physical architecture to exist"[11] may not be disregarded. The equipment constituting the architecture is usually located within the territory of a State. It is owned by the government or by corporations; it is connected to the national electric grid.[12] The integration of physical components of cyber infrastructure located within a State's territory into the "global domain" of cyberspace cannot be interpreted as a waiver of the exercise of territorial sovereignty. While, in view of the genuine architecture of cyberspace, it may be difficult to exercise sovereignty, the technological and technical problems involved do not prevent a State from exercising its jurisdiction over the cyber infrastructure located in areas in its sovereign territory. States have, in fact, continuously emphasized their right to exercise control over such infrastructure, to assert their jurisdiction over cyber activities on their territory and to protect their cyber infrastructure against transborder interference by other States or by individuals.[13]

---

inafter DoD Strategy for Operating in Cyberspace] ("DoD will treat cyberspace as an operational domain to organize, train, and equip so that DoD can take full advantage of cyberspace's potential."). *See also* U.S. Department of Defense, The Strategy for Homeland Defense and Civil Support 12 (2005), *available at* http://www.defense.gov/news/Jun2005/d20050630homeland.pdf ("The global commons consist of international waters and airspace, space, and cyberspace.").

10. *See, e.g.,* Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185.

11. Franzese, *supra* note 8, at 33.

12. *See* Joshua E. Kastenberg, *Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law*, 64 AIR FORCE LAW REVIEW 43, 64 (2009).

13. *See* DoD Strategy for Operating in Cyberspace, *supra* note 9. *See also* U.S. Department of Defense, Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, at 7–8 (2011), *available at* http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf [hereinafter Cyberspace Policy Report]; THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 12–15 (2011), *available at* http://www.

It needs to be emphasized that the applicability of the principle of sovereignty to the components of, and activities in, cyberspace is not barred by the innovative and novel character of the underlying technology. This holds true for the majority of rules and principles of customary international law. In the 2011 International Strategy for Cyberspace, the Obama administration rightly stated that the "development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[14]

This does not necessarily mean that the rules and principles of international law are applicable to cyberspace in their traditional interpretation. Because of the novel character of cyberspace, and in view of the vulnerability of cyber infrastructure, there is a noticeable uncertainty among governments and legal scholars as to whether the traditional rules and principles are sufficient to provide answers to some worrisome questions. It is, therefore, of utmost importance that States agree not only on the application of customary international law to cyberspace, but also on a common interpretation of that law that takes into due consideration the "unique attributes of networked technology."[15] As called for in the International Strategy for Cyberspace, it is necessary that governments "continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace."[16]

---

whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf [hereinafter INTERNATIONAL STRATEGY FOR CYBERSPACE].

14. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 9.

15. "Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them." *Id.*

16. *Id. See also* Cyberspace Policy Report, *supra* note 13, at 7 ("The United States is actively engaged in the continuing development of norms of responsible state behavior in cyberspace, making clear that as a matter of U.S. policy, long-standing international norms guiding state behavior also apply equally in cyberspace. Among these, applying the tenets of the law of armed conflict are critical to this vision, although cyberspace's unique aspects may require clarifications in certain areas."). The report emphasizes that the "law of armed conflict and customary international law . . . provide a strong basis to apply such norms to cyberspace governing responsible state behavior." *Id.* at 9.

C. Scope of Territorial Sovereignty in Cyberspace

The general applicability of the principle of territorial sovereignty to cyberspace encompasses that cyber infrastructure located on a State's land area, in its internal waters, territorial sea and, where applicable, archipelagic waters, and in national airspace.[17] Thus, in principle, the State is entitled to exercise control over cyber infrastructure and cyber activities in those areas. It must be kept in mind, however, that the exercise of sovereignty may be restricted by customary or conventional rules of international law, such as the immunity of diplomatic correspondence[18] and the rights of innocent passage, transit passage and archipelagic sea lanes passage.[19]

1. Geographic Scope (*Ratione Loci*)

After this identification of the areas in which the principle of territorial sovereignty applies, the first consequence is that cyber infrastructure located in those areas is protected against interference by other States. This protection is not limited to interference amounting to an unjustified use of force, to an armed attack or to a prohibited intervention.[20] Rather, because the interference constitutes an exercise of that State's jurisdiction, any activity attributable to it is considered a violation of the sovereignty of the territorial State.[21] This, *a fortiori*, holds true if the conduct has negative impacts on the integrity or function of another State's cyber infrastructure. However, not all State conduct that impacts on the cyber infrastructure of another State necessarily constitutes a violation of the principle of territorial sovereignty. If the act of interference results in inflicting material damage

17. Note that within the exclusive economic zone and on the continental shelf coastal States do not enjoy territorial sovereignty, but merely certain "sovereign rights" with respect to the natural resources in those sea areas. U.N. Convention on the Law of the Sea arts. 56, 77, Dec. 10, 1982, 1833 U.N.T.S. 3 [hereinafter LOS Convention].

18. Vienna Convention on Diplomatic Relations art. 27(1), Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95. Computers and computer networks located in the diplomatic mission are protected by Article 22.

19. LOS Convention, *supra* note 17, arts. 17–26, 37–42, 45, 52–53.

20. It is important to note that the prohibitions on the use of force and intervention only apply to States, i.e., to conduct attributable to a State. However, Article 51 of the UN Charter does not refer to the source of an armed attack giving rise to the "inherent right of self-defense." Today there is general agreement that the right applies to armed attacks by both State and non-State actors.

21. *See, e.g.*, 1 OPPENHEIM'S INTERNATIONAL LAW ¶ 123 (Robert Jennings & Arthur Watts eds., 9th ed. 1992).

to the cyber infrastructure, there seems to be a general consensus that such an act constitutes a violation of the sovereignty of the target State.[22] According to some, the damage inflicted must be not just material but severe.[23] If, however, there is no material damage or merely minor damage, it is unsettled whether that activity can be considered a violation of territorial sovereignty.[24] Those who hold that material damage is required usually cite espionage, including cyber espionage, as an example of an activity that is not a violation, because international law does not prohibit espionage. The fact that the data resident in the target system are modified by the act of intrusion is not considered sufficient to characterize cyber espionage as a prohibited violation of territorial sovereignty. It could be argued, however, that damage is irrelevant and the mere fact that a State has intruded into the cyber infrastructure of another State should be considered an exercise of jurisdiction on foreign territory, which always constitutes a violation of the principle of territorial sovereignty.

The International Strategy for Cyberspace indicates the following activities may qualify as violations of territorial sovereignty: attacks on networks; exploitation of networks; and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy.[25] While the specific natures of those activities are not indicated, it seems that the U.S. government is advocating a rather wide scope of the principle of territorial sovereignty in asserting the right to counter such acts with all necessary means, including, if necessary, the use of conventional force.

It is irrelevant whether the cyber infrastructure protected by the principle of territorial sovereignty belongs to or is operated by governmental institutions, private entities or private individuals. Moreover, such infrastructure is also protected if it is located on board aircraft, vessels or other platforms enjoying sovereign immunity.[26] The provisions of the Outer Space

---

22 *Id.*, ¶ 119.

23. This is in recognition of the fact that the use by a State of its territory very often causes negative effects on the territory of neighboring States. Since the principle of territorial integrity is not considered to be absolute in character there are good reasons to maintain that damage below the threshold of severity must be tolerated and when such damage occurs it does not violate the territorial sovereignty or integrity of the affected State.

24. Those who consider damage as relevant will not classify those activities as violations of territorial sovereignty.

25. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 12–14.

26. *See, e.g.*, LOS Convention, *supra* note 17, art. 95 ("warships on the high seas have complete immunity from the jurisdiction of any State other than the flag State"). Under Article 96 of the Convention "ships owned or operated by a State and used only for gov-

Treaty[27] and the Liability Convention[28] appear to support the conclusion that space objects operated exclusively for non-commercial government purposes also enjoy sovereign immunity.[29] While there is no treaty rule explicitly according sovereign immunity to all objects used for non-commercial government purposes, Article 5 of the UN Convention on State Immunity[30] importantly provides that a State enjoys immunity from the jurisdiction of the courts of another State with regard to its property.[31] This provision, along with the other treaties and rules just cited, provides sufficient evidence of a general principle of public international law according to which objects owned by a State or used by that State for exclusively non-commercial government purposes are an integral part of the State's sovereignty and are subject to the exclusive jurisdiction of that State if located outside the territory of another State.

"Sovereign immunity" means that any interference with an object enjoying such immunity constitutes a violation of the sovereignty of that State.[32] It must be borne in mind, however, that in times of international armed conflict the principle of sovereign immunity plays no role in relations between the belligerent States. During such conflicts objects enjoying

---

ernment non-commercial service" have the same immunity. With regard to State aircraft in international airspace, there is general consensus that they also enjoy sovereign immunity. *See* PROGRAM ON HUMANITARIAN POLICY AND CONFLICT RESEARCH, COMMENTARY ON THE HPCR MANUAL ON INTERNATIONAL LAW APPLICABLE TO AIR AND MISSILE WARFARE rule 1(cc), cmt. to rule 1(cc), ¶ 6 (2010), *available at* http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf%20[hereinafter HPCR MANUAL].

27. Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205.

28. Convention on International Liability for Damage Caused by Space Objects, Mar. 29, 1972, 24 U.S.T. 2389, 961 U.N.T.S. 187.

29. Space objects, such as satellites used for governmental and commercial purposes either by the State of registry or by that State in cooperation with a private corporation, do not enjoy sovereign immunity.

30. U.N. Convention on Jurisdictional Immunities of States and Their Property**,** G.A. Res. 59/38, annex, U.N. GAOR, 59th Sess., Supp. No. 49, U.N. Doc. A/59/49 (Dec. 16, 2004).

31. For an assessment, see David P. Stewart, *Current Developments: The UN Convention on Jurisdictional Immunities of States and Their Property*, 99 AMERICAN JOURNAL OF INTERNATIONAL LAW 194, 195–207. (2005).

32. For a first finding with regard to the sovereign immunity of warships, see the award of the Anglo-American Claims Commission in the *Jessie* case. Owners of the *Jessie*, the *Thomas F. Bayard* and the P*escawha* (Gr. Brit. v. U.S.), 6 R.I.A.A. 57 (1921), Reports: Neilsen's 479 (1926).

sovereign immunity may be destroyed if they qualify as lawful targets or are subject to seizure as booty of war[33] by the enemy's armed forces. Moreover, sovereign immunity is not limitless. For instance, the U.S. drone captured by Iran in December 2011 (allegedly downed by cyber means) had probably been in Iran's national airspace, thus violating Iran's territorial sovereignty.[34] Hence, Iran was entitled to use all necessary means, including cyber means, to terminate that violation.

Vessels and aircraft that do not exclusively serve non-commercial governmental purposes do not enjoy sovereign immunity. This doesn't mean, however, they are not protected when located in areas or spaces not covered by the territorial sovereignty of any State. While they cannot be considered an integral component of a State's sovereignty, they are included within the protective scope of that sovereignty by the link of nationality. Hence, the State of nationality exercises exclusive jurisdiction over such vessels and aircraft when they are located on the high seas or in international airspace. Accordingly, any interference with them constitutes a violation of the sovereignty of the State of nationality unless justified by a rule of international law. This also applies to space objects. It is prohibited under the Outer Space Treaty[35] to interfere with the activities of other States in the peaceful exploration and use of outer space. It is immaterial whether the space object is owned or operated by the government or by a private corporation. On the high seas and in international airspace the cyber infrastructure will regularly be located on board a vessel or aircraft. The determination of the State whose sovereignty and jurisdiction apply will depend on either following the flag-State principle[36] or on the registration of the aircraft.[37] Nationality of space objects is also determined by registration.[38]

---

33. *See* Yoram Dinstein, *Booty in Warfare*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (Rüdiger Wolfrum ed., 2012), http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e256&recno=4&author=Dinstein%20%20Yoram [hereinafter MAX PLANCK ENCYCLOPEDIA].

34. For competing views of the circumstances of the capture, see, e.g., David Axe, *Nah, Iran Probably Didn't Hack CIA's Stealth Drone*, WIRED (Apr. 24, 2012, 12:00 PM), http://www.wired.com/dangerroom/2012/04/iran-drone-hack/; Mathew J. Schwartz, *Iran Hacked GPS Signals to Capture U.S. Drone*, INFORMATION WEEK (Dec. 16, 2011, 12:30 PM), http://www.informationweek.com/security/attacks/iran-hacked-gps-signals-to-capture-us-dr/232300666.

35. *Supra* note 27.

36 LOS Convention, *supra* note 19, art. 92.

37. *See* Convention on International Civil Aviation art. 17, Dec. 7, 1944, 15 U.N.T.S. 295 ("[a]ircraft have the nationality of the State in which they are registered").

2. Exercise of Jurisdiction (*Scope Ratione Materiae*)

The second consequence of the applicability of the principle of territorial sovereignty to the components of cyberspace is the wide-ranging right of the territorial State (including the flag State and the State of registry) to exercise its jurisdiction over cyber infrastructure and over cyber activities.

The concept of jurisdiction may be understood in a broad sense as referring to a State's "lawful power to act and hence to its power to decide whether and, if so, how to act, whether by legislative, executive or judicial means. In this sense, jurisdiction denominates primarily, but not exclusively, the lawful power to make and enforce rules."[39] As has already been noted, the exercise of jurisdiction is not limited to a State's territory. For instance, a State exercises exclusive jurisdiction on board vessels flying its flag and on board aircraft registered in that State. Moreover, according to the principles of active and passive nationality, a State is entitled to exercise its jurisdiction over the conduct of individuals that occurred outside its territory. Under the universality principle, the same holds true even if neither the perpetrator nor the victim is a national of the State in question. Finally, the exercise of jurisdiction can be based upon the protective principle.[40]

For the purposes of this article, the jurisdictional bases just listed, although of importance in the cyber domain, need not be addressed; the focus will be on the scope of territorial jurisdiction.

It may be noted in this context that territorial jurisdiction does not necessarily presuppose territorial sovereignty. For instance, a State may exercise exclusive jurisdiction over territory leased or occupied.[41] Jurisdiction conferred on coastal States in their exclusive economic zones or on their continental shelves, although it may be conceived of as quasi-territorial in character, is only analogous to territorial jurisdiction *strictu sensu*, because it is limited to certain prescribed activities.

The State's right to exercise its jurisdiction, that is, to proscribe, enforce and adjudicate activities of objects and persons physically or legally present in its territory, seems to be undisputed unless otherwise limited by applica-

38. *See* Convention on Registration of Objects Launched into Outer Space, Jan. 14, 1973, 28 U.S.T. 695, 1023 U.N.T.S. 15.

39. Bernard H. Oxman, *Jurisdiction of States* ¶ 1, *in* MAX PLANCK ENCYCLOPEDIA, *supra* note 23, http://www.mpepil.com/subscriber_article?script=yes&id=/epil/entries/law-9780199231690-e1436&recno=1&author=Oxman Bernard H.

40. For a discussion of the different bases of jurisdiction, see *id.*, ¶¶ 11–45.

41. *Id.*, ¶ 15.

ble rules of international law, probably including human rights law. Cyber infrastructure located within the territory of a State, and cyber activities occurring therein, are susceptible to almost unlimited proscriptive and enforcement measures by the State. Territorial jurisdiction includes the right of a State to regulate, restrict or prohibit access to its cyber infrastructure, whether access is gained from within or without its territory. It must be reemphasized that integration of the physical components of cyber infrastructure located within a State's territory into the "global domain" of cyberspace does not constitute a waiver of the exercise of territorial sovereignty and jurisdiction. In view of the mobility of users and of cloud- or grid-distributed systems, it may often be very difficult to effectively exercise territorial jurisdiction. Still, those difficulties do not justify the conclusion that territorial jurisdiction, if applied to cyberspace, is but a "toothless tiger." To the contrary, States have regularly and quite successfully—while not always applauded—proven their willingness and determination to enforce their domestic law over a variety of cyber activities.

A specific feature of territorial jurisdiction is the so-called effects doctrine, under which a State is entitled to exercise its jurisdiction over a conduct occurring outside its territory that produces effects in its territory.[42] A useful explanation of that doctrine has been provided in a European Court of Justice judgment:

> The two undisputed bases on which State jurisdiction is founded under international law are territoriality and nationality. The former confers jurisdiction on the State in which the person or the goods in question are situated or the event in question took place. The latter confers jurisdiction over nationals of the State concerned.
>
> Territoriality itself has given rise to two distinct principles of jurisdiction:
>
> (i) subjective territoriality, which permits a State to deal with acts which originated within its territory, even though they were completed abroad;
>
> (ii) objective territoriality, which, conversely, permits a State to deal with acts which originated abroad but which were completed, at least in part, within its own territory. . . .

42. *Id.*, ¶¶ 22–26.

> [The effects doctrine] confers jurisdiction upon a State even if the conduct which produced [the effects] did not take place within its territory.[43]

Applied to the cyber domain, the effects doctrine may give rise to the exercise of jurisdiction over individuals who have conducted cyber operations against the cyber infrastructure in another State.[44]

In summary, the principle of territorial sovereignty, and the ensuing right of a State to exercise its territorial jurisdiction, applies to cyberspace insofar as the cyber infrastructure is located within its territory or on platforms over which the State exercises exclusive jurisdiction. Territorial sovereignty and territorial jurisdiction also apply to individuals present in the State and to conduct that either takes place within that territory or produces harmful effects therein. The exercise of jurisdiction under any of the recognized bases of international law is limited only if there exist explicit rules to that effect. Thus, the characteristics of cyberspace do not pose an obstacle to the exercise of territorial sovereignty and jurisdiction; they merely increase the difficulty of so doing.

D. Obligations of States in Cyberspace and the Issue of Attributability

1. Obligations of States in Cyberspace[45]

As noted previously, the principle of territorial sovereignty not only protects States by affording them exclusive rights, but also imposes obligations on them.[46] The protective scope of those obligations serves to protect the territorial sovereignty and integrity of other States.

---

43. Joined Cases C-89, 104, 114, 116–117, 125–129/85, A. Ahlström Osakeyhtio v. Comm'n, 1988 E.C.R. 5193, ¶¶ 19–21 (citation omitted), *available at* http://eur-lex.europa.eu/staging/LexUriServ/LexUriServ.do?uri=CELEX:61985CC0089:EN:HTML.

44. Hence, irrespective of the issue of attribution, Estonia would be entitled to exercise its criminal and civil jurisdiction over those individuals who conducted the distributed denial-of-service attacks against the Estonian cyber infrastructure in 2007.

45. This section does not deal with the entire spectrum of obligations States are to observe in cyberspace; therefore, the prohibition of the use of force and the issue of "armed attack" are not addressed.

46. See the references *supra* note 4 and accompanying text.

a. Duty of Prevention

The principle of territorial sovereignty entails an obligation imposed on all States to respect the territorial sovereignty of other States. As the ICJ held in its *Nicaragua* decision, "'Between independent States, respect for territorial sovereignty is an essential foundation of international relations,' and international law requires political integrity also to be respected."[47]

The obligation to respect the territorial sovereignty of other States applies to conduct that is attributable to a State. Additionally, in the *Corfu Channel* judgment, the ICJ held that respect for the territorial sovereignty of other States implies the obligation of every State "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[48] Accordingly, a State is required under international law to take appropriate actions to protect the interests of other States.[49] This obligation is not limited to prevention of "criminal acts,"[50] but applies to all activities inflicting severe damage—or that have the potential to inflict such damage—on persons and objects protected by the territorial sovereignty of the target State.[51]

In the context of cyber attacks, the duty of prevention has been correctly summarized as follows: "States have an affirmative duty to prevent cyberattacks from their territory against other states. This duty actually encompasses several smaller duties, to include . . . prosecuting attackers, and, during the investigation and prosecution, cooperating with the victim-states

47. Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S), 1986 I.C.J. 14, ¶ 202 (June 27), citing its judgment in the *Corfu Channel* case. *Corfu Channel*, *supra* note 3, at 35.

48. *Corfu Channel*, *supra* note 3, at 22.

49. United States Diplomatic and Consular Staff in Tehran (U.S. v. Iran), 1980 I.C.J. 3, ¶ 68 (May 24). *See also* YORAM DINSTEIN, WAR, AGGRESSION AND SELF-DEFENCE 215–16 (5th ed. 2011).

50. Michael N. Schmitt, *Preemptive Strategies in International Law*, 24 MICHIGAN JOURNAL OF INTERNATIONAL LAW 513, 540–41 (2003).

51. In the famous *Trail Smelter* case, the Tribunal held, *inter alia*:

> "This right (sovereignty) excludes . . . not only the usurpation and exercise of sovereign rights . . . but also an actual encroachment which might prejudice the natural use of the territory and the free movement of its inhabitants. . . ." [U]nder the principles of international law . . . no State has the right to use or permit the use of its territory in such a manner as to cause injury . . . in or to the territory of another or the properties or persons therein, when the case is of serious consequence . . . .

Trail Smelter (U.S. v. Can.), 3 R.I.A.A. 1905, 1963, 1965 (Trail Smelter Arb. Trib. 1938 & 1941).

of cyberattacks that originated from within their borders."[52] The term "cyber attack" is often understood as comprising "remote intrusions into computer systems by individuals";[53] however, mere intrusions are not included, because they do not inflict direct material harm. Rather, mere intrusions must be considered acts of espionage.[54] Since all States engage in espionage, including via cyberspace, mere intrusions into foreign computers or networks are not covered by the prohibition on cyber attacks.

The duty of prevention presupposes knowledge. This does not necessarily mean actual knowledge; it also applies to cases of presumptive knowledge. A State will have actual knowledge if its organs have detected a cyber attack originating from its territory or if it has been informed by the victim-State that a cyber attack has originated from its territory. Knowledge is to be presumed if the cyber attack can reasonably be considered to belong to a series of cyber attacks. It is important to note the ICJ has held that even if "an act contrary to international law has occurred [on a State's territory], . . . it cannot be concluded from the mere fact of the control exercised . . . over its territory . . . that that State necessarily knew, or ought to have known, of any unlawful act perpetrated therein."[55]

Although it may be concluded that the duty of prevention does not apply if the State from whose territory the acts have been initiated has neither actual nor presumptive knowledge, this conclusion is not accepted by everyone. According to some authorities, the duty of prevention should be based on a State's "actions to prevent cyberattacks in general."[56] According to this position,

> States that do not enact [stringent criminal laws and undertake vigorous law enforcement] fail to live up to their duty to prevent cyberattacks. . . . A state's passiveness and indifference toward cyberattacks make it a sanctuary state from where attackers can safely operate. When viewed in this light, a state can be held indirectly responsible for cyberattacks . . . .[57]

---

52. Matthew J. Sklerov, *Solving the Dilemma of State Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent*, 201 MILITARY LAW REVIEW 1, 62 (2009).

53. *Id.* at 14.

54. *See, e.g.*, Schaap, *supra* note 5, at 139–40. *See also supra* notes 20–24 and accompanying text.

55. *Corfu Channel*, *supra* note 3, at 18.

56. Sklerov, *supra* note 52, at 71.

57. *Id.*

However, in this author's opinion, the theoretical possibility that a State that has not enacted criminal laws—when it has not been obliged to do so under an international treaty—may become a sanctuary for cyber attackers is certainly not sufficient to justify the inapplicability of the duty of prevention's requirement for actual or presumptive knowledge.

There are, though, circumstances that may be considered as sufficient to support the assumption that a State had—or ought to have had—knowledge of the conduct. Such circumstances may exist if a cyber attack has been launched from cyber infrastructure that is under exclusive government control and that is used only for non-commercial government purposes. Provided that the origin of the cyber attack can be traced back to the government's cyber infrastructure, there may be at least a rebuttable presumption that the State should have known of that use of its territory. It is important to note that a rebuttable presumption of knowledge does not mean that the conduct is attributable to the State. If it were, it would mean that the aggrieved State would be entitled to resort to countermeasures, including, when applicable, the use of force in response to an armed attack. The rebuttable presumption is not sufficient, however, either to attribute the conduct to the State or to serve as a legal basis for countermeasures, although that might be the case if the events were occurring in the physical world. Because of the difficulty of identifying the originator of a cyber attack, attributing it to the State whose cyber infrastructure was utilized could lead to escalation since the infrastructure may have been usurped by another State or by non-State actors, such as terrorists or other criminals. Additionally, allowing countermeasures on the basis of a "knows-or-should-have-known standard" would impose far-reaching prevention obligations on States that, given the nature of the technology involved, would be difficult, if not impossible, to fulfill.

In that regard, some might be inclined to recognize the duty of prevention as applying not just to cyber attacks launched from the territory of a State, but also to cyber attacks/cyber operations that are routed through the cyber infrastructure of another State. It is unsettled, however, whether the transit of data brings into operation the obligation of prevention even if the transit State knows, or should have known, of the use of its cyber infrastructure. While extending the prevention obligation to transit of data seems simple, those so advocating fail to recognize the complexity of cyberspace. For example, the transiting data may be harmless in and of themselves, but they may be part of a larger packet. While the larger packet, the constituent parts of which may be transmitted over different nodes, may be

considered a "cyber weapon," the transit State does not know this. Additionally, in most cases it would be meaningless to oblige the transit State to take preventive action, because the data may be rerouted, thus nevertheless arriving at their destination in the target State.

b. Further Obligations

Finally, State practice seems to justify the conclusion that there is a growing readiness of States to accept obligations that are of a more general character than the obligation to refrain from harmful conduct or to prevent such conduct.

For instance, the United States has taken the position that identifying the rules and principles of international law applicable to cyberspace must be guided by applying the "broad expectations of peaceful and just interstate conduct to cyberspace."[58] The U.S. cyberspace strategy emphasizes that States "need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet"[59] and demands that the emerging norms of cyberspace behavior be guided by five criteria, including global interoperability, network stability and cybersecurity due diligence.[60] Indeed, global interoperability, which is one of the main characteristics of the Internet, can only be preserved if "States . . . act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all."[61] Network stability presupposes that States do not "arbitrarily interfere with internationally interconnected infrastructure."[62] Since cybersecurity due diligence is understood to imply that "States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse,"[63] it may be considered as reflecting the obligation of prevention as it currently exists under customary international law. It is this author's belief that each of the criteria enumerated in the International Strategy for Cyberspace may not yet have attained that status, but they may well be accepted by a considerable number of States—at least by those that

58. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 9.

59. *Id.* at 10.

60. *Id.* The remaining two criteria are "reliable access" and "multi-stakeholder governance."

61. *Id.*

62. *Id.*

63. *Id.*

are "like-minded." The criteria may, in any event, be considered to be of potentially norm-creating character, thus contributing to the progressive development of customary international law.

2. Attributability

Effective protection of territorial sovereignty in the cyber domain presupposes that particular conduct can be attributed to another State. The rather strict attributability criteria in Articles 4 to 11 of the International Law Commission's Draft Articles on State Responsibility[64] are designed for the purpose of determining State responsibility and do not necessarily preclude the application of more liberal criteria with a view to determining the origin of a cyber attack. It is, however, unclear whether States are prepared to agree on such criteria.

It is generally agreed that, in view of the architecture and characteristics of cyberspace, it is "virtually impossible to attribute a cyberattack during an attack. Although states can trace the cyberattack back to a computer server in another state, conclusively ascertaining the identity of the attacker requires an intensive, time-consuming investigation with assistance from the state of origin."[65] The cyber attacks on Estonia (2007) and on Georgia (2008) prove the correctness of this finding. The U.S. Department of Defense (DoD) has also stressed that because the "often low cost of developing malicious code and the high number and variety of actors in cyberspace make the discovery and tracking of malicious cyber tools difficult" and because "[m]ost of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action," the "interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains."[66]

Despite the difficulty of verifying the location from which an attack was launched or of identifying the attacker, DoD has announced it would

64. Draft Articles on Responsibility of States for Internationally Wrongful Acts, Rep. of the Int'l L. Comm'n, 53d Sess., UN GAOR 56th Sess., Supp. No. 10, U.N. Doc. A/56/10 (2001), *reprinted in* [2001] 2 YEARBOOK OF THE INTERNATIONAL LAW COMMISSION 26, U.N. Doc. A/CN.4/SER.A/2001/Add.1 (Part 2), *available at* http://untreaty.un.org/ilc/texts/instruments/english/draft%20articles/9_6_2001.pdf [hereinafter Draft Rules of State Responsibility].

65. Sklerov, *supra* note 52, at 7.

66. Cyberspace Policy Report, *supra* note 13, at 8.

"actively [seek] to limit the ability of such potential actors to exploit or attack the United States anonymously."[67] It is, of course, almost commonplace to state that interagency and international cooperation, as well as information sharing, is a necessary prerequisite to achieve that goal. In view of the special characteristics of cyberspace, it may well be that international law provides an obligation to cooperate if States are prepared to take attribution measures in cyberspace. It will be interesting to see whether DoD's efforts to "assess the identity of the attacker via behavior-based algorithms" and to "significantly improve its cyber forensics capabilities"[68] are successful and, what is equally important, whether other States will accept the results as sufficient evidence of the source of a cyber attack.

E. Conclusions with Regard to Territorial Sovereignty

Territorial sovereignty has proven to be an effective principle of international law that can be applied to cyberspace without far-reaching modifications if cyberspace is understood as comprising components (cyber infrastructure) located in a State's territory or that are otherwise protected by the principle of territorial sovereignty. Of course, not all aspects of conduct constituting a violation of territorial sovereignty have been clarified. For instance, there is still no consensus among States as to which cyber operations qualify as a prohibited use of force under Article 2(4) of the UN Charter or as an armed attack under Article 51. Also, the rather abstract references to "critical infrastructure" as being protected by the principle of territorial sovereignty are not very helpful in the absence of a consensus as to which objects and governmental institutions are to be considered "critical" in nature.

The concept of territorial jurisdiction also provides an effective basis for the regulation of cyber activities. States are entitled to regulate activities occurring within their territories and to enforce their domestic law. Although States enjoy an almost unlimited right to exercise their jurisdiction over cyber activities and cyber infrastructure within their territory, there is an undisputable need for an internationally agreed understanding that the Internet's functionality—the benefits it provides—would be seriously challenged if States do not exercise their jurisdiction "with respect for one another's networks and the broader Internet."[69]

67. *Id.* at 4.
68. *Id.*
69. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 10.

III. NEUTRALITY

"Neutrality" denotes the legal status of a State that is not a party to an international armed conflict. Since the rules of international law applicable to neutral States are predominantly laid down in 1907 Hague Conventions V[70] and XIII,[71] one might assume that the law of neutrality has become obsolete by desuetude or because an impartial stance vis-à-vis the aggressor and the victim of aggression would be irreconcilable with the *jus ad bellum* as codified in the UN Charter.

Indeed the international armed conflicts that have occurred since the end of the Second World War (e.g., the conflicts between Israel and Egypt, India and Pakistan, the United Kingdom and Argentina, and Iraq and Iran) might cast doubts on the continuing validity of the traditional law of neutrality. This does not establish, however, that there is no longer a law of neutrality. The very fact that some neutral governments have tried to conceal their "unneutral service" is in itself evidence those governments considered themselves bound by the law of neutrality. And those governments that openly supported one side of an international armed conflict—in most instances because the aggrieved belligerent was unable to react to their non-compliance with neutral obligations—often went to great length to justify their conduct.

States, although their conduct may not always have been in full compliance with the principle of impartiality, have, however, recognized that the traditional law of neutrality continues to apply in situations of international armed conflict.[72] The military manuals of the United States,[73] Canada,[74] the

70. Convention No. V Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, Oct. 18, 1907, 36 Stat. 2310 [hereinafter Hague V].

71. Convention No. XIII Concerning the Rights and Duties of Neutral Powers in Naval War, Oct. 18, 1907, 36 Stat. 2415 [hereinafter Hague XIII].

72. *See* Dietrich Schindler, *Transformations in the Law of Neutrality since 1945*, *in* HUMANITARIAN LAW OF ARMED CONFLICT – CHALLENGES AHEAD, ESSAYS IN HONOUR OF FRITS KALSHOVEN 367 (Astrid J.M. Delissen & Gerard J. Tanja eds., 1991); Wolff Heintschel von Heinegg, *Wider die Mär vom Tode des Neutralitätsrechts*, *in* CRISIS MANAGEMENT AND HUMANITARIAN PROTECTION, FESTSCHRIFT FÜR DIETER FLECK 221 (Horst Fischer et al. eds., 2004).

73. U.S. Navy, U.S. Marine Corps & U.S. Coast Guard, NWP 1-14M/MCWP 5-12/COMDTPUB P5800.7A, The Commander's Handbook on the Law of Naval Operations ch. 7, (2007) [hereinafter Commander's Handbook].

74. OFFICE OF THE JUDGE ADVOCATE GENERAL, DEPARTMENT OF NATIONAL DEFENCE (CANADA), LAW OF ARMED CONFLICT AT THE OPERATIONAL AND TACTICAL LEVELS ch. 13 (2003).

United Kingdom[75] and Germany,[76] as well as the *San Remo Manual*,[77] the International Law Association's Helsinki Principles[78] and the *HPCR Manual*,[79] all address the continued applicability of the law of neutrality to international armed conflicts. Thus, both State practice and writings establish the law of neutrality is alive and well.[80]

Under the UN Charter it is, at least in theory, possible to distinguish between an aggressor and the victim of aggression. This does not mean that States are entitled to unilaterally absolve themselves from the obligations of the law of neutrality and take a "benevolent" attitude in favor of the alleged victim of an unlawful use of force.[81] If, however, the UN Security Council has decided upon preventive or enforcement measures under Chapter VII of the UN Charter, the scope of applicability of the law of neutrality will be reduced considerably and the 1907 Hague Conventions will be inapplicable.[82] Under Articles 25 and 103 of the UN Charter, States

---

75. UNITED KINGDOM MINISTRY OF DEFENCE, THE MANUAL OF THE LAW OF ARMED CONFLICT (2004). It is important to note that the *UK Manual* does not contain a chapter specifically devoted to the law of neutrality; however, its continuing validity is expressly recognized in paragraph 1.42, and chapters 12 (Air Operations) and 13 (Maritime Warfare) contain rules on neutral States, neutral aircraft and neutral vessels.

76. FEDERAL MINISTRY OF DEFENCE (GERMANY), HUMANITARIAN LAW IN ARMED CONFLICTS MANUAL ch. 11 (1992) [hereinafter GERMAN MANUAL].

77. SAN REMO MANUAL ON INTERNATIONAL LAW APPLICABLE TO ARMED CONFLICTS AT SEA ¶¶ 7–26, 28–32, 34–36, 60, 67–71, 74–75, 85–88, 92–94, 106, 108–10, 113–16, 118–20, 122–27, 130, 132–35, 141, 146–47, 151–57, 161, 165–68, 179–83 (Louise Doswald-Beck ed., 1995).

78. Committee on Maritime Neutrality, International Law Association, *Helsinki Principles on the Law of Maritime Neutrality, May 30, 1998*, *in* INTERNATIONAL LAW ASSOCIATION, REPORT OF THE 68TH CONFERENCE TAIPEI, 1998, at 496 (1998), *reprinted in* THE LAWS OF ARMED CONFLICTS: A COLLECTION OF CONVENTIONS, RESOLUTIONS AND OTHER DOCUMENTS 1425 (Dietrich Schindler & Jiri Toman eds., 4th ed. 2004) [hereinafter Helsinki Principles].

79. HPCR MANUAL, *supra* note 26, sec. X.

80. *See* Heintschel von Heinegg, *supra* note 72, at 232.

81. Wolff Heintschel von Heinegg, *"Benevolent" Third States in International Armed Conflicts: The Myth of the Irrelevance of the Law of Neutrality*, *in* INTERNATIONAL LAW AND ARMED CONFLICT: EXPLORING THE FAULTLINES 543 (Michael N. Schmitt & Jelena Pejic eds., 2007).

82. *See* SAN REMO MANUAL, *supra* note 77, ¶¶ 7–9; HPCR MANUAL, *supra* note 26, rule 165; Helsinki Principles, *supra* note 78, ¶ 1.2. For the powers of the UN Security Council and the obligations of UN member States, see DINSTEIN, *supra* note 49, at 308–15. For a restrictive approach to the powers of the UN Security Council, see ERIKA DE WET, THE CHAPTER VII POWERS OF THE UNITED NATIONS SECURITY COUNCIL 133–74 (2004).

not parties to an international armed conflict are obliged to comply with UN Security Council decisions and, in any event, to refrain from activities interfering with or impeding the exercise of enforcement operations authorized by resolutions implementing those decisions.[83]

In view of the foregoing, this section starts from the premise that, subject to decisions by the UN Security Council under Chapter VII of the UN Charter, the traditional law of neutrality applies to States not parties to an international armed conflict. It will first explore whether, and to what extent, that body of law is applicable to cyberspace. It will then identify the obligations of belligerents and of neutrals with regard to military operations in cyberspace.

A. Applicability of the Law of Neutrality to Cyberspace

The continuing validity of the core principles and rules of the law of neutrality in an international armed conflict characterized by the use of traditional kinetic weapons is beyond question. But when it comes to hostilities and hostile acts conducted in or through cyberspace, some might reject their applicability. Indeed, if cyberspace is considered to be a new "fifth dimension," a "global common" that "defies measurement in any physical dimension or time space continuum,"[84] it could be rather difficult to maintain that the law of neutrality applies. If it is acknowledged, however, that cyberspace "requires a physical architecture to exist,"[85] many of the difficulties can be overcome.

The law of neutrality serves a dual protective purpose. On the one hand, it is to protect the territorial sovereignty of neutral States and their nationals against the harmful effects of the ongoing hostilities. On the other hand, it aims to protect belligerent interests against interference by neutral States and their nationals to the benefit of one belligerent and to the detriment of the other. Thus, the rules and principles of the law of neutrality aim to prevent escalation of an ongoing international armed conflict "[by] regulating the conduct of belligerents with respect to nations not participating in the conflict, [by] regulating the conduct of neutrals with re-

83. For an analysis of the effects of UN Charter Article 103, see Rudolf Bernhardt, *Article 103*, *in* 2 THE CHARTER OF THE UNITED NATIONS: A COMMENTARY 1292, 1295–1302 (Bruno Simma et al. eds., 2d ed. 2002).

84. WINGFIELD, *supra* note 6, at 17.

85. Franzese, supra note 8, at 33. *See also supra* notes 10–13 and accompanying text.

spect to belligerents, and [by] reducing the harmful effects of such hostilities on international commerce."[86]

Applied in the cyber context, it is safe to conclude that the law of neutrality protects the cyber infrastructure located in the territory of a neutral State or that resides in sovereign immune platforms and other objects used by the neutral State for non-commercial government purposes. Thus, belligerents are under an obligation to respect the sovereignty and inviolability of States not parties to the international armed conflict by refraining from any harmful interference with the cyber infrastructure located in neutral territory. Neutral States must remain impartial and may not engage in cyber activities that support the military actions of one belligerent to the detriment of the opposing belligerent. Moreover, they are obliged to take all feasible measures to terminate an abuse of the cyber infrastructure located within their territory or on their sovereign immune platforms by the belligerents.

Because they are based upon a teleological interpretation of the law of neutrality, some may question these findings; however, they are supported not only by the majority of authors addressing the issue of neutrality in the cyber context,[87] but also by State practice. For instance, DoD has taken the position that "long-standing international norms guiding state behavior—in times of peace and conflict—also apply in cyberspace."[88] DoD's Cyberspace Policy Report, *inter alia*, emphasizes that "applying the tenets of the law of armed conflict [is] critical."[89] The report also addresses activities "taking place on or through computers or other infrastructure located in a neutral third country."[90] The applicability of the law of neutrality to cyberspace has also been acknowledged in the recent *HPCR Manual*.[91] Since that manual has been endorsed by a considerable number of governments, it may be considered a restatement of the existing law, and as reflecting the consensus of those States on the issues it addresses.

Of course, the rules of the traditional law of neutrality, while in principle applicable to cyberspace, may require clarification—or even modifica-

86. Commander's Handbook, *supra* note 73, ¶ 7.1.

87. *See, e.g.*, Kastenberg, *supra* note 12, at 56–64; Graham H. Todd, *Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition*, 64 AIR FORCE LAW REVIEW 65, 90–91 (2009); George K. Walker, *Information Warfare and Neutrality*, 33 VANDERBILT JOURNAL OF TRANSNATIONAL LAW, 1079, 1182–84 (2000).

88. DoD Strategy for Operating in Cyberspace, *supra* note 9, at 9.

89. Cyberspace Policy Report, *supra* note 13, at 8.

90. *Id.*

91. HPCR MANUAL, *supra* note 26, rule 168(b).

tion—because of the unique characteristics of cyberspace.[92] Still the "law of armed conflict and customary international law . . . provide a strong basis to apply such norms to cyberspace governing responsible state behavior."[93]

B. Obligations of Belligerents

Under the law of neutrality belligerents are obliged to respect the inviolability of neutral territory; hence, they are prohibited from conducting hostilities, from exercising belligerent rights or establishing bases of operations within neutral territory. These prohibitions are laid down in international treaties[94] and they are considered customary in character.[95]

1. No Harmful Interference with Neutral Cyber Infrastructure

It follows from the foregoing that cyber infrastructure located within the territory of a neutral State is protected against harmful interference by the belligerents. It does not matter whether the cyber infrastructure is owned or exclusively used by the government, corporations or private individuals. Neither does the protection depend upon the nationality of the owner. In view of the principle of sovereign immunity, the same protection applies to cyber infrastructure located on neutral State ships and State aircraft or in diplomatic premises.

The prohibition on harmful interference with neutral cyber infrastructure is not limited to cyber attacks *strictu sensu*, i.e., to cyber operations that cause, or are expected to cause, damage, destruction, death or injury. Rather, it is to be understood as also comprising all activities, whether kinetic or cyber, that either have a negative impact on their functionality or make their use impossible. In other words, it is prohibited to engage in "the use of network-based capabilities . . . to disrupt, deny, degrade, manipulate, or

92. Cyberspace Policy Report, *supra* note 13, at 7.

93. *Id.* at 8.

94. Hague V, *supra* note 70, arts. 1–3; Hague XIII, *supra* note 71, arts. 1–2, 5.

95. *See* Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶¶ 1108, 1149; SAN REMO MANUAL, *supra* note 77, ¶ 15; HPCR MANUAL, *supra* note 26, rule 166. *See also* Hague Rules of Aerial Warfare arts. 39, 40, 42, 47, Feb. 19, 1923, 32 AMERICAN JOURNAL OF INTERNATIONAL LAW SUPPLEMENT 12 (1938) (not in force), *reprinted in* THE LAWS OF ARMED CONFLICTS, *supra* note 78, at 315 [hereinafter 1923 Hague Air Rules].

destroy information resident in computers and computer networks, or the computers and networks themselves"[96] of a neutral State.

Of course, as previously noted, mere intrusion into neutral cyber infrastructure is not covered by this prohibition, because international law does not prohibit espionage. It must be borne in mind, however, that the principle of territorial sovereignty includes the prohibition on exercising jurisdiction on foreign territory;[97] therefore a cyber operation characterized as an exercise of jurisdiction would be in violation of the sovereignty of the target State. That prohibition is of a general character and thus not part of the law of neutrality *strictu sensu*.

2. Exercise of Belligerent Rights and Use of Cyber Infrastructure in Neutral Territory

Belligerents are prohibited from using neutral cyber infrastructure for the purpose of exercising belligerent rights against the enemy or against others. It is important to note that the term "belligerent rights" is not limited to cyber attacks, but refers to all measures a belligerent is entitled to take under the law of armed conflict against the enemy belligerent, enemy nationals or the nationals of neutral States.[98] This prohibition follows from the very object and purpose of the law of neutrality, i.e., to prevent an escalation of the international armed conflict.

In view of its object and purpose, this prohibition also applies to the exercise of belligerent rights through the use of neutral cyber infrastructure that enjoys sovereign immunity, that is, infrastructure located outside neutral territory used by a neutral State for exclusively non-commercial government purposes. It is not as certain that the prohibition also applies to the use of cyber infrastructure owned by a private corporation or an individual located outside neutral territory. In such a situation, however, the cyber infrastructure can be considered as contributing to the enemy's mili-

96. Schaap, *supra* note 5, at 127.

97. *Lotus, supra* note 1, at 18–19 ("Now the first and foremost restriction imposed by international law upon a State is that—failing the existence of a permissive rule to the contrary—it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention.").

98. Such actions comprise detention, requisitions, capture and interception.

tary action and the opposing belligerent would be entitled to treat it as a lawful military objective.[99]

Moreover, a belligerent may not make use of its own cyber infrastructure for military purposes if it is located on neutral territory. It is irrelevant whether the cyber infrastructure has been "erected" prior to or after the outbreak of the international armed conflict. This prohibition follows from Article 3 of Hague V, according to which

> belligerents are . . . forbidden to:
>
> (a) Erect on the territory of a neutral Power a wireless telegraphy station or other apparatus for the purpose of communicating with belligerent forces on land or sea;
>
> (b) Use any installation of this kind established by them before the war on the territory of a neutral Power for purely military purposes, and which has not been opened for the purpose of public messages.

3. Exceptions to the Prohibition on Exercising Belligerent Rights

As has been discussed, the prohibition on exercising belligerent rights through the use of neutral cyber infrastructure must be interpreted in the light of the unique characteristics of cyberspace.[100] Cyberspace is an "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[101] Given the interdependence and ubiquity of cyberspace and its components, it would be almost impossible for a belligerent to prevent the routing of malicious data packages through the cyber infrastructure located in the territory of a neutral State even though it is ultimately aimed against the enemy. Therefore, it seems to be

---

99. For the definition of lawful military objectives, see Article 52(2) of the 1977 Additional Protocol I to the 1949 Geneva Conventions. This definition reflects customary international law. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts, June 8, 1977, 1125 U.N.T.S. 3.

100. *See supra* note 84 and accompanying text.

101. Dictionary of Military and Associated Terms, *supra* note 5. See also the definition by Schaap, *supra* note 5, at 126 ("cyberspace" is a "domain characterized by the use of [computers and other electronic devices] to store, modify, and exchange data via networked systems and associated physical infrastructures").

logical and perhaps even cogent to apply Article 8 of Hague V to cyber operations and cyber attacks conducted by a belligerent against its enemy. Article 8 provides: "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."

Doubts have been articulated in the literature as to whether Article 8 has any application to cyberspace.[102] That position is based on the assumption that a cyber operation conducted through neutral cyber infrastructure is to be considered as originating from neutral territory. Article 8, however, only applies to communications. It is Article 2 of Hague V that prohibits belligerents, *inter alia*, from moving "munitions of war or supplies across the territory of a neutral Power." If the distinction between mere communications through and passage of "munitions of war . . . across" were applied to cyberspace, any transmission of a cyber weapon through neutral cyber infrastructure would constitute a violation of the law of neutrality, whereas mere communications would not. Indeed, there are some indications that States share that view. For instance, in 1999 DoD's Office of General Counsel arrived at the conclusion that "[t]here is nothing in this agreement [i.e., Hague V] that would suggest that it applies to systems that generate information, rather than merely relay communications."[103] It is interesting to note that DoD seems prepared to apply Article 8 to cyberspace, although it would limit its applicability to mere communications, i.e., to cyber operations that do not amount to a cyber attack.

Articles 2 and 8 of Hague V are based on the assumption that a neutral State exercises full and effective control over its entire territory, but not over installations and objects used for communications purposes. The different degrees of feasible and effective control must also be taken into account in the cyber context. In recognition of the nature of cyberspace, the *HPCR Manual* provides: "[W]hen Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[104]

---

102. Kastenberg, *supra* note 12, at 56–64; Todd, *supra* note 87, at 90–91.

103. Office of General Counsel, U.S. Department of Defense, An Assessment of International Legal Issues in Information Operations 10 (May 1999), *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

104. HPCR MANUAL, *supra* note 26, rule 167(b).

The *HPCR Manual* does not distinguish between mere communications on the one hand and the transmission of cyber weapons on the other. The phrase "use for military purposes" is sufficiently broad to cover both. This seems to be a reasonable adaptation of the traditional rules of the law of neutrality to cyberspace. Because of the complexity and interdependence of contemporary networks, such as the Internet, it is impossible to exercise the control necessary to effectively interfere with communications over such networks. This is underlined by the fact that most such communications are often neither traceable nor predictable since they will be transmitted over lines of communications and routers passing through various countries before reaching their ultimate destinations. These realities being taken into account, under this view, the mere fact that military communications, including cyber attacks, have been transmitted via the cyber infrastructure of a neutral State is not considered to constitute a violation of that State's neutral obligations.

It is acknowledged, despite the attractiveness of the *HPCR Manual*'s approach for both belligerents and neutral States, it is unclear that such a far-reaching adaptation of Article 8 to cyber operations conducted for military purposes will ultimately be accepted as reflective of contemporary customary international law. Modern State practice, especially the cyber operations during the 1999 Kosovo campaign, the conflicts in Afghanistan (2001) and Iraq (2003), and the armed conflict between Georgia and Russia (2007), provides insufficient evidence to establish that a cyber operation, including the transmission of cyber weapons through neutral cyber infrastructure, does not violate the neutrality of the States through which the transmissions passed. First, there is no open-source information establishing that the cyber operations amounted to cyber attacks or that they had been routed through neutral cyber infrastructure. Second, the distributed denial-of-serve attacks against Georgia, according to the position taken by this author, do not qualify as cyber attacks *strictu sensu* and, therefore, cannot be assimilated to the transit of "munitions of war" under Article 2 of Hague V. On the other hand, the DoD's Cyberspace Policy Report suggests the United States considers every "malicious cyber activity" as a violation of the law of neutrality, irrespective of whether they have been launched from or merely transmitted through "computers or other infrastructure located in a neutral third country."[105]

105. Cyberspace Policy Report, *supra* note 13, at 8.

What is clear today is that the use of neutral cyber communications by a belligerent does not constitute a violation of neutrality even though it serves military purposes. It is less clear, however, that this is also true if the cyber operation qualifies as a "malicious cyber activity" or cyber attack. We will return to this issue in the context of the consequences of a violation of the law of neutrality by neutral States.

C. Obligations of Neutral States

The law of neutrality, in view of its object and purpose,[106] poses obligations not only upon the belligerents, but also on neutral States. Setting aside the duty of impartiality,[107] a neutral State's obligations may be divided into three categories: (1) a prohibition on allowing or tolerating the exercise of belligerent rights in its territory, (2) an obligation to terminate (and probably to prevent) a violation of its neutrality by a belligerent and (3) an obligation to accept the enforcement of the law of neutrality by the aggrieved belligerent.

1. The Prohibition on Allowing or Tolerating the Exercise of Belligerent Rights

According to Article 5 of Hague V, a "neutral Power must not allow any of the acts referred to in Articles 2 to 4 to occur in its territory." Accordingly, a neutral State may not allow or tolerate the exercise of belligerent rights that utilize either the cyber infrastructure located within its territory or that located outside its territory, provided that the neutral State exercises exclusive control over it.[108]

The different interpretations of Article 8 of Hague V may have far-reaching consequences. Under the *HPCR Manual* approach,[109] a malicious cyber activity routed through neutral cyber infrastructure that is, for example, a component of the Internet would not constitute a prohibited exercise

106. *See supra* note 86 and accompanying text.

107. Hague V, *supra* note 70, art. 9. Article 9 of Hague XIII provides a "neutral Power must apply impartially to the two belligerents the conditions, restrictions, or prohibitions made by it." Accordingly, restrictions on military communications via its cyber infrastructure must be applied impartially by the neutral State. *See also* SAN REMO MANUAL, *supra* note 77, ¶ 19.

108. *See supra* notes 98–105 and accompanying text.

109. HPCR MANUAL, *supra* note 26, rule 167(b).

of belligerent rights. Therefore, a neutral State allowing or tolerating such an activity would not violate its obligations under the law of neutrality. If, however, the *HPCR Manual* approach is not considered to reflect customary international law, the transmission of a cyber attack through neutral infrastructure would have to be considered a prohibited exercise of belligerent rights, and the neutral State that knowingly allows or tolerates the transmission would be in violation of its neutral obligations.

But even if the latter approach is taken, the consequences are less grave than one may assume. Contrary to the position of one author,[110] the use of the term "allow" in the traditional rule presupposes knowledge by the neutral State. That will be the case if it has detected a malicious cyber activity/cyber attack or if it has been informed in a sufficiently credible manner that the activity/attack has originated from, or has been transmitted through, the State's cyber infrastructure. Such knowledge will result in a violation of the law of neutrality by the neutral State only if the malicious cyber activity continues. In most cases, cyber attacks will occur at such high speed that the knowledge that it has occurred is available only after the event. *Ex post facto* knowledge hardly suffices to justify a claim of a violation of the law of neutrality.

Even if constructive—as opposed to actual—knowledge is considered sufficient to establish a violation of the obligation that too would not result in noticeable changes in the manner in which the law of neutrality applies. Constructive knowledge means that the neutral State should have known of the malicious activity, but, again, in most cases such knowledge would not necessarily result in a violation of neutral obligations, because of the speed of cyber operations.

The analysis would probably be different if, as a result of the prohibition of allowing the exercise of belligerent rights, neutral States were obliged to actively monitor cyber activities originating from or transiting through their cyber infrastructure; however, it is far from settled that such an obligation exists. The *San Remo Manual*, in addressing physical violations of neutral territory, provides that a "neutral State must take such measures . . . including the exercise of surveillance, as the means at its disposal allow, to prevent the violation of its neutrality by belligerent forces."[111] It is not likely, however, that States, especially those that defend the freedom of Internet communications, will agree that the obligation to monitor land areas

110. Kastenberg, *supra* note 12, at 57.

111. SAN REMO MANUAL, *supra* note 77, ¶ 15.

and certain sea areas applies equally to the cyber infrastructure located in their territory.

2. Obligation to Terminate and to Prevent a Violation of Neutrality

According to the traditional law of neutrality, neutral States are obliged to terminate an exercise of belligerent rights and any other violation of their neutrality by one of the belligerents.[112] This obligation is part of contemporary customary international law.[113]

The obligation to enforce neutral status against violations by the belligerents is not absolute in character, but is limited to what is feasible. In other words, the neutral State is obliged to use all means reasonably available to it to terminate an exercise of belligerent rights occurring within its territory.[114] The applicable standard is not objective but rather subjective; it depends on the means and capabilities factually available to the neutral State. It must be emphasized that, subject to feasibility, the duty to enforce neutral status entails an obligation to use all means necessary, including the use of force, to effectively terminate an unlawful exercise of belligerent rights. The belligerent against which such measures are applied may not consider them as a hostile act, that is, it is obliged to tolerate them as a lawful action by the neutral State carrying out its neutrality obligations.[115]

The obligation to terminate an ongoing violation of neutrality presupposes knowledge—actual or constructive—by the neutral State.[116] It is quite probable that the neutral State is unaware of an abuse of its cyber infrastructure. But even if such actual or constructive knowledge existed, it would in most cases be futile to demand the neutral State take measures against the belligerent, because the cyber operation triggering the duty to terminate has been completed.

---

112. *Id.*, ¶¶ 18, 22; HPCR MANUAL, *supra* note 26, rule 168(a). *See also* 1923 Hague Rules, *supra* note 95, arts. 42, 47.

113. SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶ 1109.

114. SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3; GERMAN MANUAL, *supra* note 76, ¶ 1109.

115. Hague V, *supra* note 70, art. 10; HPCR MANUAL, *supra* note 26, rule 169; 1923 Hague Air Rules, *supra* note 95, art. 48.

116. *See supra* note 104 and accompanying text.

Limiting a neutral's obligation to the termination of ongoing cyber activities is considered by some authors to be insufficient. They assert that a neutral State is also obliged to take all feasible measures to prevent an exercise of belligerent rights, that is, to act before it occurs.[117] At first glance, that position seems to reflect customary international law, because some military manuals expressly refer not only to an obligation to terminate an ongoing violation of neutrality, but also to a duty to prevent an exercise of belligerent rights within neutral territory.[118] It is, however, doubtful whether the use of the term "prevent" is meant to establish an obligation vis-à-vis future violations of neutrality. But even if that were the case, the duty to prevent would be limited to violations of neutral territory and national airspace. It is far from clear that States are willing to accept a prevention requirement, because that implies an obligation to continuously monitor cyber activities originating from or transiting through their cyber infrastructure. Additionally, monitoring would be of limited utility since, as has been shown, the identification of the malicious nature of data packages transiting through a network would in most cases be extremely difficult, if not impossible.

Therefore, there are good reasons for rejecting a prospective duty of prevention. If there is such an obligation, it exists only with regard to activities within neutral territory that could be assimilated to those covered by Article 8 of Hague XIII.[119] For instance, the authorities of a neutral State may have actual or constructive knowledge of the activities of a group of hackers that has been employed by a belligerent government to develop a cyber weapon to be used against the enemy. In such a situation the neutral State would be obliged to take all feasible measure to prevent the departure of the cyber weapon from its territory.

---

117. Kastenberg, *supra* note 12, at 56–64.

118. SAN REMO MANUAL, *supra* note 77, ¶ 15; HPCR MANUAL, *supra* note 26, rule 168(a); Commander's Handbook, *supra* note 73, ¶ 7.3.

119. A neutral Government is bound to employ the means at its disposal to prevent the fitting out or arming of any vessel within its jurisdiction which it has reason to believe is intended to cruise, or engage in hostile operations, against a Power with which that Government is at peace. It is also bound to display the same vigilance to prevent the departure from its jurisdiction of any vessel intended to cruise, or engage in hostile operations, which had adapted entirely or partly within the said jurisdiction for use in war.

3. Consequences of Non-compliance by Neutral States

The law of neutrality provides that if a neutral State fails to terminate an exercise of belligerent rights or other violations of its neutrality by one belligerent, the other belligerent is entitled to take those measures necessary to terminate the violation.[120] The right of the aggrieved belligerent to enforce the law of neutrality comes into operation if the neutral State is either unwilling or unable to comply with its obligation to terminate a violation of its neutral status by the enemy. This right is a specific form of a countermeasure, i.e., a measure that would be unlawful if it was not taken in response to a violation of international obligations by the target State.[121] Its object and purpose are (1) to induce the neutral State to comply with its obligations and (2) to enable the aggrieved belligerent to preserve its security interests. Not every violation of neutrality by one belligerent justifies a resort to countermeasures by the other belligerent. The violation in question must have a negative impact on the legitimate security interests of that belligerent. This will not be the case if a belligerent takes measures against a neutral State's cyber infrastructure that do not provide a military advantage vis-à-vis the other belligerent. In that case, the right to respond to the violation is reserved to the neutral State and the exercise of that right is probably subject to a *de minimis* exception.

When the neutral State does not act to terminate a violation of its neutrality, the aggrieved belligerent is not entitled to immediately resort to the exercise of countermeasures. In that regard, the *San Remo Manual* provides: "If the neutral State fails to terminate the violation of its neutral waters by a belligerent, the opposing belligerent must so notify the neutral State and give that neutral State a reasonable time to terminate the violation by the belligerent."[122] An immediate response by the aggrieved belligerent is lawful only if (1) the violation constitutes a serious and immediate threat to the security of that belligerent, (2) there is no feasible and timely alternative and (3) the enforcement measure taken is necessary to respond to the threat posed by the violation.[123]

---

120. Commander's Handbook, *supra* note 73, ¶ 7.3; SAN REMO MANUAL, *supra* note 77, ¶ 22; HPCR MANUAL, *supra* note 26, rule 168(b). For those who believe there is also an obligation to prevent a violation, the other belligerent would also have the right to act if the neutral State fails to do so.

121. *See* Draft Articles on State Responsibility, *supra* note 64, arts. 22, 49–54.

122. SAN REMO MANUAL, *supra* note 77, ¶ 22.

123. *Id. See also* HPCR MANUAL, *supra* note 26, rule 168(b).

The aggrieved belligerent's right to enforce the law of neutrality certainly applies to cyberspace if a malicious cyber activity originates from the territory of a neutral State.[124] DoD seems to be prepared to take such enforcement measures if it is determined a neutral State is aware of the malicious cyber activity. The Cyberspace Policy Report indicates that in making that determination the following will be taken into account:

> The nature of the malicious cyber activity; the role, if any, of the third country; the ability and willingness of the third country to respond effectively to the malicious cyber activity; and the appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstances.[125]

This is a clear restatement of the rules of the law of neutrality, providing evidence of DoD's willingness to apply those rules to conduct in cyberspace.

D. Conclusions with Regard to the Law of Neutrality

It has been shown that the traditional law of neutrality is, in principle, applicable to cyberspace. This is especially true of belligerent cyber operations that qualify as an exercise of belligerent rights within neutral territory. As with the principle of territorial sovereignty, the special characteristics of cyberspace do not, as such, pose an obstacle to the application of that law. Certainly, however, there remains an urgent need for clarification and even adaptation of the traditional law. In view of the interdependence of the networks through which data are transmitted and the potentially disastrous effects on critical infrastructure subjected to a cyber attack, there is a high probability that belligerent States will take measures, including the use of kinetic force, against neutral States and their cyber infrastructure if they determine vital security interests are at stake. Such measures have the potential to jeopardize the essential object and purpose of the law of neutrality—preventing escalation of an international armed conflict.

124. *See* Cyberspace Policy Report, *supra* note 13, at 8.
125. *Id.*

IV. FINAL THOUGHTS

The U.S. government has taken helpful first steps in the identification of the applicable rules of international law and their interpretation in the context of the challenges brought about by the specific characteristics of cyberspace. Other governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence.[126] The five criteria identified in the International Strategy for Cyberspace should be accepted by other States because they are of a potentially norm-creating character and assist in clarifying the scope of existing rules and principles of international law applicable to the cyber domain. Moreover, governments should cooperate with a view to improving their capabilities in the area of cyber forensics. Such cooperative efforts are necessary not only in order to identify attackers, but also to establish a more effective deterrent of malevolent States and non-State actors.

126. INTERNATIONAL STRATEGY FOR CYBERSPACE, *supra* note 13, at 10.