2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Legal Implications of Territorial Sovereignty in Cyberspace

Wolff Heintschel von Heinegg
Faculty of Law
Europa-Universität
Frankfurt (Oder), Germany
heinegg@europa-uni.de

Abstract: The principle of territorial sovereignty applies to cyberspace and it protects the cyber infrastructure located within a State's territory. States are prohibited to interfere with the cyber infrastructure located in the territory of another State. This certainly holds true if the conduct is attributable and if it inflicts (severe) damage on the integrity or functionality of foreign cyber infrastructure. Moreover, States have the obligation not to allow knowingly their territory to be used for acts that violate the territorial sovereignty of another State. It is, however, unsettled whether there is a rebuttable presumption of knowledge if the cyber attacks were launched from the government cyber infrastructure of the State of origin.

States have a right to exercise their territorial jurisdiction over cyber activities within their territories. However, the characteristics of cyberspace and the necessity to preserve the functionality of the Internet call for consensual limitations of an exercise of territorial jurisdiction. The U.S. International Strategy for Cyberspace has the potential of guiding governments in order to either progressively develop international law or to specify existing norms of international law.

The attribution of cyber attacks to a given State continues to be a challenging problem. Nevertheless, States should continue to improve their capabilities in the area of cyber forensics. The U.S. Department of Defense Cyberspace Policy Report is to be considered a valuable contribution to that effect.

Keywords: *territorial sovereignty, exercise of jurisdiction, cyber infrastructure, obligations of States in cyberspace*

1. INTRODUCTION

The question whether traditional rules and principles of international law apply to conduct in cyberspace is far from new. Still, at least in Europe governments do not seem to have shown a specific interest in a clarification of the applicable norms of international law before the cyber attacks on Estonia in 2007 and on Georgia in 2008 although the discussion in the United

States of America had been underway since the end of the 20th century. Of course, it is a positive development that the issue of the applicability of (customary) international law to cyberspace has gained the attention it deserves. Less positive is the mystification of cyberspace as a 'fifth dimension' or as a 'fifth domain' that according to some is considered so novel that it eludes the traditional rules and principles of international law. Such an exaggeration of cyberspace is neither justified nor necessary and it therefore does not justify the various calls for 'new norms of international law' specifically designed for cyberspace. International law as it currently stands need not capitulate in view of the challenges brought about by cyberspace and the technology it is based upon. States seem to agree that customary international law is, in principle, applicable to cyberspace although there may be a need for a consensual adaptation to the specific characteristics of cyberspace.

The present paper will, for obvious reasons, not address the entire spectrum of customary international law that may have an impact on State conduct in cyberspace. Rather, it will explore whether and to what extent the rights and duties derived from the principle of territorial sovereignty do apply to cyberspace. It will be shown that the principle of territorial sovereignty applies to certain components of cyberspace and that the specific rights and obligations flowing from that principle have not become obsolete for the mere fact that cyberspace is characterized as a fifth dimension or as part of the global commons.

2. GENERAL CHARACTERISTICS OF TERRITORIAL SOVEREIGNTY

Irrespective of the various theories on the legal function of territory[1] there is widespread agreement that according to the principle of territorial sovereignty a State exercises full and exclusive authority over its territory.[2] Max Huber, in the Palmas Island Arbitration award, has affirmed this general principle as follows: "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".[3] According to the International Court of Justice "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations".[4] Territorial sovereignty (or: 'full and exclusive authority') therefore implies that, subject to applicable customary or conventional rules of international law, the respective 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. Territorial sovereignty protects a State against any form of interference by other States. While such interference may imply the use of force, that aspect is not dealt with here.

It must borne in mind that territorial sovereignty does not merely afford protection to States but it also imposes obligations on States, especially the "obligation to protect within the territory

1 For a discussion of the various theories on the legal function of territory see Santiago Torres Bernárdez, 'Territorial Sovereignty', in Encyclopedia of Public International Law Vol. IV, p. 823 at p. 824 *et seq*. (ed. by R. Bernhardt, Amsterdam et al. 2000).

2 See, *inter alia*, The *Lotus*, PCIJ Ser. A, No. 10, at p. 18 *et seq*. (1927); *Free Zones of Upper Savoy and Gex Case*, PCIJ Ser. A/B, No. 46, p. 166 *et seq*. (1932).

3 2 RIAA p. 829 at p. 838.

4 ICJ, *The Korfu Channel Case (Merits)*, ICJ Rep., 1, at p. 35 (1949).

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."[5]

3. 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".[6] 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."[7] It is true that cyberspace is characterized by anonymity and ubiquity.[8] Therefore it seems logical to assimilate it to the high seas, international airspace and outer space[9], i.e., to consider it a 'global common' or legally a *res communis omnium*.[10] However, these characterizations merely justify the obvious conclusion that cyberspace in its entirety is not subject to the sovereignty of a single State or of a group of States. In view of its characteristics it is immune from appropriation.

Despite of the correct classification of 'cyberspace as such' as a *res communis omnium* State practice gives sufficient evidence that cyberspace, or rather: components thereof, is not immune from sovereignty and from the exercise of jurisdiction. On the one hand, States have exercised, and will continue to exercise, their criminal jurisdiction vis-à-vis cyber crimes[11] and they continue to regulate activities in cyberspace. On the other hand, it is important to bear in mind that "cyberspace requires a physical architecture to exist".[12] The respective equipment is usually located within the territory of a State. It is owned by the government or by corporations. It is

5 Max Huber in the *Palmas Arbitration*, *supra* note 3, at p. 839. In his Separate Opinion in the *Korfu 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", ICJ Rep., p. 43 (1949).

6 Joint Chiefs of Staff, Joint Pub. 1-02, Dept. of Defense Dictionary of Military and Associated Terms, at 41 (12 April 2001). See also the definition by Arie J. Schaap, 'Cyber Warfare Operations: Development and Use under International Law', 64 AFLR, 121-173, at 126 (2009), who defines 'cyberspace' as 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".

7 Thomas Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, at 17 (Aegis Research Corp. 2000).

8 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, at 12 (2006), available at http://www.allacademic.com/meta/p98069_index.html.

9 For an analysis to that effect see Patrick W. Franzese, 'Sovereignty in Cyberspace: Can It Exist?', 64 AFLR 1-42, at 18 *et seq*. (2009).

10 U.S Department of Defense, *Strategy for Operating in Cyberspace* (available at http://www.defense.gov/news/d20110714cyber.pdf): "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*, at 12 (2005:) "The global commons consist of international waters and airspace, space, and cyberspace."

11 It suffices to refer to the Council of Europe Convention on Cybercrime of 23 November 2001, E.T.S. No.185.

12 Franzese, supra note 9, at 33.

connected to the national electric grid.[13] The integration of physical components, i.e., 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. In view of the genuine architecture of cyberspace it may be difficult to exercise sovereignty. Still, the technological and technical problems involved do not prevent a State from exercising its sovereignty, especially its criminal jurisdiction, to the cyber infrastructure located in areas covered by its territorial sovereignty.

States have continuously emphasized their right to exercise control over the cyber infrastructure located in their respective territory, to exercise their jurisdiction over cyber activities on their territory, and to protect their cyber infrastructure against any trans-border interference by other States or by individuals.[14]

It needs to be emphasized that the applicability of the principle of sovereignty to the said 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 that do apply to cyberspace and to cyber activities. The U.S. President, in the 2011 International Strategy for Cyberspace, has clearly 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."[15]

This does not necessarily mean that the said rules and principles are applicable to cyberspace in their traditional interpretation. In view of the novel character of cyberspace and in view of the vulnerability of cyber infrastructure and cyber components there is a noticeable uncertainty amongst governments and legal scholars as to whether the traditional rules and principles of customary international law are sufficiently apt to provide the desired answers to some worrying questions. It is, therefore, of utmost importance that States not only agree on the principal application of customary international law to cyberspace but also on a common interpretation that takes into due consideration the "unique attributes of networked technology".[16] Hence it is necessary that governments "continue to work internationally to forge consensus regarding how norms of behavior apply to cyberspace".[17]

13 See Joshua E. Kastenberg, 'Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law', 64 AFLR, 43-64, at 64 (2009).

14 See the *Strategy for Operating in Cyberspace*, *supra* note 10. See further 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 4 *et seq*. (November 2011), available at http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.; U.S. President, *International Strategy for Cyberspace*, at 12 *et seq*. (May 2011).

15 *Ibid*., at 9.

16 *Ibid*.: "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."

17 *Ibid*. See also the Cyberspace Policy Report, *supra* note 14, 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." At p. 9 the Report emphasizes that the "law of armed conflict and customary international law, however, provide a strong basis to apply such norms to cyberspace governing responsible state behavior."

4. SCOPE OF TERRITORIAL SOVEREIGNTY IN CYBERSPACE

The basic applicability of the principle of territorial sovereignty to cyberspace entails that the cyber infrastructure located on the land territory, in the internal waters, in the territorial sea, and, where applicable, in the archipelagic waters, or in the national airspace is covered by the respective State's territorial sovereignty.[18] Hence, in principle, the State is entitled to exercise control over that cyber infrastructure and over cyber activities in those areas. It may not be left out of consideration, however, that the exercise of sovereignty may be restricted by customary or conventional rules of international law, such as the immunity of diplomatic correspondence[19] or the rights of innocent passage, transit passage, and archipelagic sea lanes passage.[20]

A. Ratione loci

The first consequence of the above findings is that the cyber infrastructure located in areas covered by the territorial sovereignty is protected against interference by other States. This protection is not limited to activities amounting to an unjustified use of force, to an armed attack or to a prohibited intervention.[21] Rather, any activity attributable to another State, e.g. because it constitutes an exercise of that State's jurisdiction, is to be considered a violation of the sovereignty of the territorial State.[22] This also holds true if the attributable conduct has negative impacts on the integrity or functionality of the cyber infrastructure. It is important to note that not every 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 to the cyber infrastructure located in another State, there seems to be a sufficient consensus that such an act constitutes a violation of the territorial sovereignty of the target State.[23] In this context it must be conceded that according to some the damage inflicted must be severe.[24] If, however, there is no or merely minor material damage to the cyber infrastructure it is not really settled whether that activity can be considered a violation of territorial sovereignty.[25] The usual example given is espionage, including cyber espionage because international law lacks a prohibition of espionage. The fact that the data resident in the target system are modified by the act of intrusion is not considered sufficient to qualify it a prohibited violation of territorial sovereignty. It could, however, be argued that

18 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 a view to the natural resources in those sea areas.

19 Vienna Convention on Diplomatic Relations, Article 27(1). Note that the computers and computer networks located in the diplomatic mission are protected by Article 22.

20 United Nations Convention on the Law of the Sea of 30 April 1982 (UN Doc. A/CONF. 62/122 of 7 October 1982), Articles 17 *et seq*., 37 *et seq*., 45, 52, and 53.

21 It is important to note that the prohibitions of 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. Today, there is general agreement that the right of self-defence also applies to armed attacks by non-State actors.

22 See, *inter alia*, R. Jennings/A. Watts (eds.), Oppenheim's International Law, Vol. I, para. 123, 9th ed., Jennings & Watts (eds.) (Harlow 1992).

23 *Ibid*., para. 119.

24 This is due to the fact that the use by a State of its territory very often causes negative effects on the territory of neighbouring 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 does not violate the territorial sovereignty (integrity) of the affected State.

25 Those who consider damage as relevant will not qualify such acts as violations of territorial sovereignty.

damage is irrelevant and that the mere fact that foreign State organs have intruded into the cyber infrastructure of another State is to be considered an exercise of jurisdiction on foreign territory that always constitutes a violation of the principle of territorial sovereignty.

According to the U.S. International Strategy for Cyberspace the following activities may qualify as violations of U.S. territorial sovereignty: attacks on networks, exploitation of networks, and other hostile acts in cyberspace that threaten peace and stability, civil liberties and privacy.[26] While the respective acts are not specified it seems that the U.S. government is advocating a rather wide scope of the principle of territorial sovereignty because it asserts the right to respond to such acts with all necessary means, including, if necessary, the use of (conventional) force.

As regards the cyber infrastructure thus protected by the principle of territorial sovereignty it is irrelevant whether it belongs to, or is operated by, governmental institutions, private entities or private individuals.

Moreover, such infrastructure is equally protected if it is located onboard aircraft, vessels or other platforms enjoying sovereign immunity. Article 95 LOSC[27] provides that "warships on the high seas have complete immunity from the jurisdiction of any State other than the flag State". According to Article 96 LOSC the same applies to "ships owned or operated by a State and used only for government non-commercial service". As regards state aircraft in international airspace there is general consensus that they enjoy sovereign immunity as well.[28] The Outer Space Treaty[29] and the Liability Convention[30] seem to justify the conclusion that space objects operated for non-commercial government purposes also enjoy sovereign immunity.[31] While there is no treaty rule explicitly according sovereign immunity to all objects used for non-commercial government purposes it is of importance that according to Article 5 of the UN Convention on State Immunity[32] a State enjoys immunity from the jurisdiction of the courts of another State with regard to its property.[33] This rule and the other rules just referred to give 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 they are subject to the exclusive jurisdiction of that State if they are 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 the State using the object for non-commercial government purposes.[34] It

26 International Strategy for Cyberspace, *supra* note 14, at 12 *et seq*.
27 *Supra* note 20.
28 See HPCR Manual on Air and Missile Warfare, Rule 1 (cc) and accompanying commentary, para. 6, available at http://ihlresearch.org/amw/Commentary%20on%20the%20HPCR%20Manual.pdf.
29 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies of 10 October 1967, UN GA. Res. 2222 (XXII).
30 Convention on International Liability for Damage Caused by Space Objects of 1 September 1972, UN GA Res. 2777 (XXVI).
31 Note that 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.
32 UN Convention on Jurisdictional Immunities of States and Their Property of 2 December 2004, UN GA Res. 59 (XXXVIII).
33 For an assessment see David P. Stewart, 'The UN Convention on Jurisdictional Immunities of States and Their Property', 99 AJIL 194-211, at 195 et seq. (2005).
34 For a first finding with regard to the sovereign immunity of warships see the Award of the Anglo-American Claims Commission, *The Jessie, The Thomas F. Bayard and The Pescawha*, Nielsen's Report, 479 *et seq*. (1926).

must be borne in mind, however, that in times of an international armed conflict the principle of sovereign immunity plays no role in the relations between the belligerent States. Then, objects enjoying sovereign immunity may be destroyed (if they qualify as lawful targets) or they are subject to seizure (booty of war)[35] by the respective enemy armed forces. Moreover, sovereign immunity is not limitless. For instance, the U.S. drone downed by Iran (allegedly by cyber means) had been in Iran's national airspace and it, thus, violated Iran's territorial sovereignty. Hence, Iran was entitled to use all necessary means, including cyber means, to terminate that violation.

Vehicles that do not serve exclusively non-commercial governmental purposes do not enjoy sovereign immunity. This, however, does not mean that they are not protected when located in areas or spaces that are 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 into the protective scope of that sovereignty by the link of nationality. This means, that the respective State of nationality exercises exclusive jurisdiction over such objects when they are located on the high seas or in international airspace. Accordingly, any interference with such objects constitutes a violation of the sovereignty of the State of nationality (unless justified by a rule of public international law). This also applies to space objects. It is prohibited, under the Outer Space Treaty[36], 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 and the determination of the State whose sovereignty and jurisdiction applies will depend on either the flag State principle[37] or on the national markings the aircraft carries.[38] That is different in outer space because satellites will in most cases have to be considered as qualifying as 'cyber infrastructure', i.e., without reference to a carrying platform. As in the case of aircraft, nationality of space objects is determined by registration.[39]

B. Exercise of Jurisdiction (Scope Ratione Materiae)

The second consequence of the applicability of the principle of territorial sovereignty to 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 wide sense and 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".[40] As already noted above, the exercise of jurisdiction is not limited to a State's territory. For instance, a State exercises exclusive jurisdiction onboard vessels flying its flag and onboard aircraft registered in that State. Moreover, according to the principles of active and of passive nationality, a State is

35 See Yoram Dinstein, 'Booty of War', in: MPEPIL, available at http://www.mpepil.com.
36 *Supra* note 29.
37 Article 92 LOSC, *supra* note 20.
38 According to Article 17 of the Convention on International Civil Aviation (Chicago Convention) of 7 December 1944, "[a]ircraft have the nationality of the State in which they are registered".
39 See the Convention on Registration of Objects Launched into Outer Space of 15 September 1976, UN GA Res. 34/68.
40 Bernard H. Oxman, 'Jurisdiction of States', para. 1, in: MPEPIL, available at http://www.mpepil.com.

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 are nationals of the State in question. Finally, the exercise of jurisdiction can be based upon the protective principle.[41]

For the purposes of this paper that deals with the principle of territorial sovereignty the forms of jurisdiction just referred to, although of importance in the cyber domain, need not be elaborated upon. Therefore, 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.[42] It may also be noted that the jurisdiction conferred on coastal States in their Exclusive Economic Zone or on their continental shelf, 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 activities.

For the purposes of this paper, it suffices to concentrate on a State's right to exercise its jurisdiction (i.e., to prescribe, enforce and adjudicate) over objects and persons physically (or legally) present in its territory. It seems to be undisputed that, unless limited by applicable 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 prescriptive and enforcement measures by the respective State. Territorial jurisdiction includes the right of a State to regulate, restrict or prohibit access to its cyber infrastructure either within its territory or from outside that territory. It must be re-emphasized that integration of physical components, i.e., 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 and jurisdiction. In view of the mobility of users and of cloud or grid distributed systems it may very often be 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 vis-à-vis all kinds of cyber activities.

A specific feature of territorial jurisdiction is the so-called 'effects doctrine' according to which a State is entitled to exercise its jurisdiction over a conduct that does not take place within its territory but that produces (harmful) effects in that territory.[43] A useful explanation of that doctrine has been provided by the European Attorney-General:

> "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:

41 For a discussion of the different bases of jurisdiction see *ibid*., paras. 18 *et seq*.
42 *Ibid*., para. 15.
43 *Ibid*., paras. 22 *et seq*.

(i) subjective territoriality, which permits a State to deal with acts which are originated within its territory, even though 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.
[The effects doctrine] confers jurisdiction upon a State even if the conduct which produced [the effects] did not take place within the territory."[44]

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.[45]

In sum, it can be held that the principle of territorial sovereignty and the ensuing right of a State to exercise its territorial jurisdiction apply to cyberspace insofar as the cyber infrastructure within the territory (or on platforms over which the State exercises exclusive jurisdiction) is concerned. The same holds true for individuals present in that territory or for conduct that either takes place within that territory or that produces (harmful) effects thereon. The exercise of jurisdiction under any of the recognized bases under international law is limited only if there exist explicit rules to that effect. The characteristics of cyberspace do not pose an obstacle to the exercise of territorial sovereignty and jurisdiction.

5. OBLIGATIONS OF STATES IN CYBERSPACE AND THE ISSUE OF ATTRIBUTABILITY

A. Obligations of States in Cyberspace

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 dealt with here. However, as noted above, the principle of territorial sovereignty does not only protect States by affording them exclusive rights but it also imposes obligations on them.[46] The protective scope of those obligations aims at the protection of the territorial sovereignty and integrity of other States.

Duty of Prevention

In view of its fundamental character 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 the Nicaragua Case: "'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]

First of all, the obligation to respect the territorial sovereignty of other States applies to conduct that is attributable to a State. However, according to the Korfu Channel Judgment, respect for

44 ECJ, *Ahlström and others v. Commission (In re Wood Pulp Cartel)*, joint cases 89/85, 104/85, 114/85, 116-17/85 and 125-9/85, 96 ILR 148 et seq. (1994).

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

46 See the references *supra* note 5 and accompanying text.

47 ICJ, *Case concerning Military and Paramilitary Activities in and against Nicaragua (Merits)*, ICJ Rep. 1986, 14, at 106, para. 202, referring to its Judgment in the *Korfu Channel Case*, ICJ Rep. 1949, 35.

the territorial sovereignty of other States also 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 acts in order to protect the interests of other States.[49] This obligation is not limited to "criminal acts"[50] but applies to all activities inflicting (severe) damage, or having the potential of inflicting such damage, on persons and objects protected by the (territorial) sovereignty of the target State.[51]

The duty of prevention, in the context of cyber attacks, 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 of cyberattacks that originated from within their borders."[52]

It must be borne in mind that the term 'cyber attack' is often understood as comprising "remote intrusions into computer systems by individuals".[53] However, mere intrusions have to be excluded because they do not inflict direct (material) harm. Rather, intrusions must be considered acts of espionage that are not prohibited under public international law.[54] Since all States engage in espionage, including via the cyberspace, mere intrusions into foreign computers or networks are not covered by the prohibition.

The duty of prevention presupposes knowledge. This does not necessarily mean actual knowledge. The duty also applies to cases of presumptive knowledge. A State will have actual knowledge if its organs have detected a cyber attack originating from that State's territory or if that State 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 that the International Court of Justice has held that even if "a State on whose territory […] an act contrary to international law has occurred, may be called upon to give an explanation […] 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]

Hence, there are good reasons to conclude that the duty of prevention does not apply if the State from whose territory the respective acts have been committed has neither actual nor

48 ICJ, *The Korfu Channel Case (Merits)*, ICJ Rep. 1949, 1, at 22.

49 ICJ, *Case concerning United States Diplomatic and Consular Staff in Tehran*, ICJ Rep. 1980, 3, at 32 *et seq*., para. 68. See also Yoram Dinstein, *War, Aggression and Self-Defence*, at 206 (4th ed., Cambridge 2004).

50 Michael N. Schmitt, 'Preemptive Strategies in International Law', 24 Mich.J.Int'l.L., 513, at 540 *et seq*. (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. […] under 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 […]"; RIAA Vol. III, 1905, at 1963 *et seq*.

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 MLR 1-85, at 62 (Fall 2009).

53 *Ibid*., at 14.

54 See, *inter alia*, Schaap, *supra* note 6, at 139 *et seq*.

55 ICJ, *The Korfu Channel Case (Merits)*, ICJ Rep. 1949, 1, at 18.

presumptive knowledge. Such a conclusion is however, not necessarily generally accepted.

According to a position held in the literature 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 vigorous law enforcement] fail to live up with 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] However, the mere theoretical possibility of a State that has not enacted criminal laws (and not being obliged to do so under an international treaty) becoming a sanctuary for cyber attackers is certainly not sufficient to justify the applicability of the duty of prevention.

There is, however, a situation that may be considered as sufficient for the assumption that the respective State had, or ought to have had, knowledge of the conduct. Such a situation may exist if a cyber attack has been launched from cyber infrastructure that is under exclusive government control and that is used for non-commercial government purposes only. Provided that the origin of, for instance, a cyber attack can be traced back to such government cyber infrastructure, there may at least be a rebuttable presumption that the respective 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 respective conduct is, thus, attributable to the State. That would mean that the aggrieved State would be entitled to resort to counter-measures, including, where applicable, to the use of force. However, the rebuttable presumption as such is not sufficient to either attribute the conduct to the State or to serve as a legal basis for counter-measures although that might be the case with a view to events occurring in the physical world. In cyberspace such an approach could lead to an escalation and it would certainly impose on States too far-reaching obligations because the government cyber infrastructure may have been usurped by another State or by non-State actors, such as terrorists or other criminals.

Without prejudice to the problem of attributing a cyber attack to a State it may not be left out of consideration that the duty of prevention applies only if and insofar as the cyber attack has been launched from the territory of a given State. Despite of the complexity of cyberspace some might be inclined to recognize the duty of prevention to apply also to cyber attacks/cyber operations that are routed through the cyber infrastructure of another State. It is, however, unsettled whether the transit of data through another State brings into operation the obligation of prevention even if the transit State knows, or should have known, of the use of the cyber infrastructure located on its territory. On the one hand, the respective data may only be parts of a data packet. While the packet as such may be considered a 'cyber weapon', its constituent parts may be transmitted over different nodes. On the other hand, in most cases it would be meaningless to oblige the transit State to take preventive action because the data may be rerouted and may therefore nevertheless arrive at their destination.

Further Obligations

Finally, it may be added that 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.

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

For instance, the U.S President has taken the position that identifying the rules and principles of international law applicable to cyberspace must be guided by the "broad expectations of peaceful and just interstate conduct to cyberspace."[58] The U.S. President 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 he demands that the emerging norms are guided by five criteria, including global interoperability, network stability and cyber security due diligence.[60] Indeed, global interoperability is one of the main characteristics of the Internet and it can only be preserved if "States […] act within their authorities to help ensure the end-to-end interoperability of an Internet accessible to all". Network stability presupposes that States do not "arbitrarily interfere with internationally interconnected infrastructure". Since cyber security 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", it may be considered as already being part of customary international law, i.e., reflective of the obligation of prevention discussed above. According to the position taken here the criteria enumerated in the International Strategy for Cyberspace may not yet have the status of customary international law but they may well be accepted by a considerable number of States – at least by those that are 'like-minded'. The criteria may in any event be considered as being of a potentially norm-creating character, thus contributing to the progressive development of customary international law.

B. Attributability

An effective protection of territorial sovereignty in the cyber domain presupposes that a given conduct can be attributed to another State. Of course, the rather strict criteria of attributability in Articles 4 to 11 of the ILC's Draft Articles on State Responsibility[61] are designed for the purpose of State responsibility and they 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."[62] 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 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. Most of the technology used in this context is inherently dual-use, and even software might be minimally repurposed for malicious action." In conclusion, the DoD admits that the "interconnected nature of cyberspace poses significant challenges for applying some of the legal frameworks developed for specific physical domains."[63]

58 International Strategy for Cyberspace, *supra* note 14, at 9.
59 *Ibid*., at 10.
60 *Ibid*. The remaining two are reliable access and multi-stakeholder governance.
61 Draft Articles on Responsibility of States for Internationally Wrongful Acts, UN GA Res. 56/82 of 12 December 2001.
62 Sklerov, *supra* note 52, at 7.
63 Cyberspace Policy Report, *supra* note 14, at 8.

Despite of the difficulty of verifying the location from which an attack was launched or of identifying the attacker, the DoD has announced it would "actively seek to limit the ability of such potential actors to exploit or attack the United States anonymously"[64] It is, of course, almost a commonplace that inter-agency and international cooperation as well as information sharing are a necessary prerequisite to achieve that goal. In view of the special characteristics of cyberspace it may well be stated that international law provides an obligation to cooperate if States are prepared to take measures in cyberspace. It will be interesting to see whether the DoD's efforts to "assess the identity of the attacker via behavior-based algorithms" and to "significantly improve its cyber forensics capabilities"[65] will be successful and, what is equally important, accepted by other States as conclusive or sufficient evidence of the source of a cyber attack.

6. CONCLUSIONS

Territorial sovereignty has proven to be a powerful and effective norm of international law that can be applied to cyberspace without far-reaching modifications if cyberspace is understood as comprising components – or: cyber infrastructure – that is located in a State's territory or otherwise protected by the principle of territorial sovereignty. It may not be forgotten that this finding does not imply that all aspects of the protection of territorial sovereignty have thus been clarified. For instance, there still is no consensus among States as to which cyber operations qualify as a prohibited use of force according to Article 2 (4) of the UN Charter or as an armed attack under Article 51. The rather abstract references to 'critical infrastructure' are not very helpful if there is no consensus as to which objects and institutions are to be considered 'critical' in nature.

Equally effective is the concept of territorial jurisdiction. Accordingly, States are entitled to regulate cyber activities occurring within their territories and to enforce their domestic law. Although States enjoy an almost unlimited right to exercise their territorial jurisdiction with a view to cyber activities and cyber infrastructure within their territories there is an undisputable need for an internationally agreed understanding that the Internet's functionality and thus the benefits it entails would be seriously challenged if States do not exercise their territorial jurisdiction "with respect for one another's networks and the broader Internet".[66] Therefore, the five criteria identified by the U.S. President in the International Strategy for Cyberspace should be taken up by other governments. They are of a potentially norm-creating character and they would assist in a clarification of the existing rules and principles of international law that apply to the cyber domain.

Finally, 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 for a more effective deterrence of malevolent States and non-State actors.

64 *Ibid*., at 4 *et seq*.
65 *Ibid*.
66 International Strategy for Cyberspace, *supra* note 14, at 10.