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

Neutrality in Cyberspace

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

Abstract: The primary object and purpose of the law of neutrality is to protect the (territorial) sovereignty of neutral States and to prevent an escalation of an international armed conflict. Despite of the unique characteristics of cyberspace there is widespread agreement that that body of law applies to cyber operations taken against, or by use of, cyber infrastructure that is located within the territory of neutral States.
Belligerents must respect the inviolability of neutral States and they are prohibited to exercise belligerent rights within their territory. It is, however, not yet sufficiently clear whether that prohibition also applies to (malicious) cyber activities transmitted through neutral cyber infrastructure.
Neutral States are prohibited to allow the exercise of belligerent rights within their territory. Moreover, they are under an obligation to take all feasible measures to terminate such exercise. Again, it is unclear whether neutral States are also obliged to prevent a future exercise of belligerent rights.
If a neutral State is unwilling or unable to comply with its obligation to terminate (or to prevent) a violation of its neutral status, the aggrieved belligerent is entitled to enforce the law of neutrality, subject to proportionality.

Keywords: *neutrality, neutral cyber infrastructure, prohibition of exercising belligerent rights within neutral territory, enforcement of neutral obligations*

1. INTRODUCTION

'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 the 1907 Hague Conventions V[1] and XIII[2] one might be inclined to 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 occurred after the end of the Second World War (e.g., the conflicts between Israel and Egypt, India and Pakistan, United Kingdom and Argentina, or Iraq and Iran) might cast doubts on the continuing validity of the traditional law

1 Convention (V) Respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, The Hague, 18 October 1907, 2 AJIL Supp. 117-127 (1908).

2 Convention (XIII) Concerning the Rights and Duties of Neutral in Naval War, The Hague, 18 October 1907, 2 AJIL Supp. 202-216 (1908).

of neutrality. It may, however, not be left out of consideration that States, although their conduct may not always have been in compliance with the principle of impartiality, have recognized that the traditional law of neutrality continues to apply to contemporary international armed conflicts.[3] It suffices to refer to the most recent military manuals of the USA[4], Canada[5], the United Kingdom[6] and Germany[7] as well as to the San Remo Manual[8], the ILA Helsinki Principles[9] and the HPCR Manual[10]. Hence, the law of neutrality is well alive.[11]

Under the UN Charter it is, at least in theory, possible to distinguish between an aggressor and the victim of aggression. This, however, does not mean that States are entitled to unilaterally absolve themselves from the obligations of the law of neutrality and to take a 'benevolent' attitude in favour of the alleged victim of an unlawful use of force.[12] 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.[13] In view of Articles 25 and 103 of the UN Charter States 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 under such resolution.[14]

Hence, the present paper 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

3 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*, 367-386 (ed. by A.I.M. Delissen/G.J. Tanja, Dordrecht 1991); Wolff Heintschel von Heinegg, 'Wider die Mär vom Tode des Neutralitätsrechts', in: *Crisis Management and Humanitarian Protection, Festschrift für Dieter Fleck*, 221-241 (ed. by H. Fischer et al., Berlin 2004).

4 The Commander's Handbook on the Law of Naval Operations, NWP 1-14M, Chapter 7 (Newport 1997).

5 Law of Armed Conflict at the Operational and Tactical Levels, Chapter 13 (2003).

6 UK Ministry of Defence, *The Manual of the Law of Armed Conflict*, (Oxford 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 para. 1.42 and Chapters 12 (Air Operations) and 13 (Maritime Warfare) contain rules on neutral States, neutral aircraft and neutral vessels.

7 The Federal Ministry of Defence of the Federal Republic of Germany, Humanitarian Law in Armed Conflicts – Manual, Chapter 11 (Bonn 1992).

8 San Remo Manual on International Law Applicable to Armed Conflicts at Sea, paras. 14 *et seq*., available at: http://www.icrc.org. See also (ed.), San Remo Manual on International Law Applicable to Armed Conflict at Sea (ed. by L. Doswald Beck, Cambridge 1995).

9 ILA, *Helsinki Principles on the Law of Maritime Neutrality*, ILA Report of the Sixty-Eighth Conference, at 497 et seq. (London 1998).

10 Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare, Section X (Bern 2009).

11 See Heintschel von Heinegg (supra note 3), at 232 *et seq*.

12 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*, 543-568 (ed. by Michael N. Schmitt and Jelena Pejic, Leiden / Boston 2007).

13 See San Remo Manual (supra note 8), paras. 7-9; HPCR Manual (supra note 10), Rule 165; Helsinki Principles (supra note 9), para. 1.2. For the powers of the UN Security Council and the obligations of UN member States see Yoram Dinstein, *War, Aggression and Self-Defence*, at 279 *et seq*., 289 *et seq*. (4th ed., Cambridge 2005). 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*, at 133 *et seq*. (Oxford 2004).

14 For an analysis of the effects of Article 103 UN Charter see Rudolf Bernhardt, 'Article 103', in: The Charter of the United Nations. A Commentary, Vol. II, 1292-1302, at 1295 *et seq*. (ed. by Bruno Simma, 2nd ed., Oxford 2002).

that body of law is applicable to cyberspace (2.) and it will then identify the obligations of belligerents (3.) and neutrals (4.) with regard to (military) operations in cyberspace.

2. APPLICABILITY OF THE LAW OF NEUTRALITY TO CYBERSPACE

The continuing validity of the core principles and rules of the law of neutrality cannot be doubted in the course of an international armed conflict that is characterized by the use of traditional (kinetic) weapons. But when it comes to hostilities and hostile acts conducted in or through cyberspace one might be inclined to reject their applicability. Indeed, if cyberspace is considered to be a new '5th dimension', a 'global common', that "defies measurement in any physical dimension or time space continuum"[15] it could be rather difficult to maintain that the law of neutrality applies. If we acknowledge, however, that cyberspace "requires a physical architecture to exist"[16], many of the difficulties can be overcome.

The law of neutrality serves a double 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 at the protection of belligerent interests against any 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 at preventing an escalation of an ongoing international armed conflict "in regulating the conduct of belligerents with respect to nations not participating in the conflict, in regulating the conduct of neutrals with respect to belligerents, and in reducing the harmful effects of such hostilities on international commerce."[17]

Applied to the cyber context it is safe to conclude that the law of neutrality protects the cyber infrastructure that is located within the territory of a neutral State or that profits from the sovereign immunity of platforms and other objects used by the neutral State for non-commercial government purposes.[18] Hence, 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 within neutral territory. Neutral States must remain impartial and they may not engage in cyber activities that support the military action of one belligerent and that are to the detriment of the other 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 any of the belligerents.

The correctness of these findings might be doubted because they are based upon a teleological interpretation of the law of neutrality alone. However, they are supported not only by the

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

16 Patrick W. Franzese, 'Sovereignty in Cyberspace: Can It Exist?', 64 AFLR 1-42, at 33 (2009).

17 NWP 1-14M (*supra* note 4), para. 7.1.

18 Territory consists of the land territory, the internal waters, the territorial sea and, where applicable, the archipelagic waters of a neutral State as well as the airspace above those areas. Platforms and objects enjoying sovereign immunity include warships, military aircraft and diplomatic premises and communication devices.

majority of authors dealing with the issue of neutrality in the cyber context[19] but also by State practice. For instance, the U.S. Department of Defense (DoD) has taken the position that "long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace."[20] The DoD Cyberspace Policy Report, *inter alia*, emphasizes that "applying the tenets of the law of armed conflict are critical".[21] The Report also addresses activities "taking place on or through computers or other infrastructure located in a neutral third country".[22] It may be added in this context that the applicability of the law of neutrality to cyberspace has also been acknowledged in the recent HPCR Manual.[23] Since that Manual has been endorsed by a considerable number of governments it may be considered as a restatement of the existing law and as reflecting the consensus of States on the issues dealt with in the Manual.

Of course, the rules of the traditional law of neutrality, while in principle applicable to cyberspace, may require clarifications or even modifications because of the unique characteristics of cyberspace.[24] Still, the "law of armed conflict and customary international law […] provide a strong basis to apply such norms to cyberspace governing responsible state behavior."[25]

3. OBLIGATIONS OF BELLIGERENTS

According to the law of neutrality belligerents are obliged to respect the inviolability of neutral territory. Hence, they are prohibited to conduct hostilities, to exercise belligerent rights or to establish bases of operations within neutral territory. These prohibitions are laid down in international treaties[26] and they are considered as customary in character.[27]

A. No Harmful Interference with Neutral Cyber Infrastructure

It follows from the foregoing that the cyber infrastructure located within the territory of a neutral State is protected against any harmful interference by the belligerents. It does not matter whether the respective cyber infrastructure is owned (or exclusively used) by the government, by corporations or by private individuals. Neither does the protection depend upon the nationality of the owner. In view of the principle of sovereign immunity the same

19 See, *inter alia*, Joshua E. Kastenberg, 'Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law', 64 AFLR 43-64, at 56 et seq. (2009); Graham H. Todd, 'Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition', *ibid*. 65-102, at 90 *et seq*.; George K. Walker, 'Information Warfare and Neutrality', 33 Vanderbilt J.Trans.L., 1079-1202, at 1182 *et seq*.

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

21 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 et seq. (November 2011), available at: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

22 *Ibid*., at 8.

23 *Supra* note 10, Rule 168 (b).

24 Cyber Policy Report (supra note 21), at 7.

25 *Ibid*., at 8.

26 Articles 1, 2, and 3 of the 1907 Hague Convention V (supra note 1); Articles 1, 2 and 5 of the 1907 Hague Convention XIII (*supra* note 2).

27 See NWP 1-14M (*supra* note 4), para. 7.3; German Manual (*supra* note 7), paras. 1108, 1149; San Remo Manual (*supra* note 8), para. 15; HPCR Manual (*supra* note 10), Rule 166. See also Articles 39, 40, 42 and 47 of the Rules of Aerial Warfare, The Hague, 1923, 32 AJIL Suppl. 12-56 (1938).

protection applies to every cyber infrastructure located on neutral state ships and state aircraft or in diplomatic premises.

The prohibition of harmfully interfering with neutral cyber infrastructure is not limited to cyber attacks, 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 the 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 destroy information resident in computers and computer networks, or the computers and networks themselves"[28], of a neutral State.

Of course, mere intrusion into neutral cyber infrastructure is not covered by this prohibition because international law lacks a prohibition of espionage. It must be borne in mind that the principle of territorial sovereignty includes the prohibition of exercising jurisdiction on foreign territory.[29] Hence, a cyber operation that may be characterised as an exercise of jurisdiction would be in violation of the sovereignty of the target State. However, that prohibition is of a general character and thus not part of the law of neutrality *strictu sensu*.

B. Exercise of Belligerent Rights and Use of Belligerent Cyber Infrastructure

Belligerents are prohibited to use 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 that it 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.[30] 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 by the use of neutral cyber infrastructure that enjoys sovereign immunity because it is used by the organs of a neutral State for exclusively non-commercial government purposes and that is located outside neutral territory. It is not equally clear whether the prohibition also applies to the use (or: abuse) of cyber infrastructure located outside neutral territory that is owned by a private corporation or individual. Be that as it may. In such a situation the respective cyber infrastructure may be considered as contributing to the enemy's military action and the opposing belligerent would therefore be entitled to treat it as a lawful military objective.[31]

Moreover, a belligerent may not make use of its cyber infrastructure for military purposes if it is located on neutral territory. It is irrelevant whether the cyber infrastructure has been 'erected'

28 Arie J. Schaap, 'Cyber Warfare Operations: Development and Use under International Law', 64 AFLR, 121-173, at 127 (2009).

29 Permanent Court of International Justice, Judgment No. 9, *The Case of the S.S. "Lotus"*, PCIJ Ser. A No. 10 (1927), at 18: "La limitation primordiale qu'impose le droit international à l'Etat est celle d'exclure – sauf l'existence d'une règle permissive contraire – tout exercice de sa puissance sur le territoire d'un autre Etat. Dans ce sens, la juridiction est certainement territoriale; elle ne pourrait être exercée hors du territoire, sinon en vertu d'une règle permissive découlant du droit international coutumier ou d'une convention."

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

31 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.

prior to or after the outbreak of the international armed conflict. This prohibition follows from Article 3 of the 1907 Hague Convention 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."

C. Exceptions to the Prohibition of Exercising Belligerent Rights?

As already mentioned, the prohibition of exercising belligerent rights by the use of neutral cyber infrastructure must be interpreted in the light of the unique characteristics of cyberspace.[32] Cyberspace is an "interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".[33] In view of the interdependence and the 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 within the territory of a neutral State although it is ultimately aimed against the enemy.

Therefore it seems to be logical and perhaps even cogent to apply Article 8 of the 1907 Hague Convention V to cyber operations and to 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."

Although some doubts have been articulated in the literature as to whether Article 8 Hague V was at all applicable to cyberspace[34], that position would not justify a total rejection of Article 8 because it is based on the assumption that a cyber operation conducted through neutral cyber infrastructure is to be considered as originating from neutral territory. Then, and only then, it would have to be considered an exercise of belligerent rights from neutral territory.

It must be borne in mind, however, that Article 8 only applies to communications and that Article 2 of Hague Convention V prohibits belligerents, *inter alia*, to "move […] munitions of war or supplies across the territory of a neutral Power". If the distinction between mere communications and a passage of "munitions of war" were applied to cyberspace any transmission of a 'cyber weapon' through neutral cyber infrastructure would constitute a violation of the law of neutrality. Indeed, there are some indications that States will share that view. For instance, the

32 *Supra* note 24 and accompanying text.
33 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 Schaap, *supra* note 28, at 126, 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".
34 Kastenberg (*supra* note 19), at 56 et seq.; Todd (*supra* note 19), at 90 et seq.

Office of General Counsel of the U.S. DoD, in 1999, arrived at the conclusion that "[t]here is nothing in this agreement [i.e., Hague Convention V] that would suggest that it applies to systems that generate information, rather than merely relay communications."[35] It is interesting to note that the U.S. DoD seems to be prepared to apply Article 8 of the 1907 Hague Convention V to cyberspace, although it would limit its applicability to mere communications, i.e., to cyber operations that do not amount to a cyber attack.

It may, however, not be left out of consideration that Articles 2 and 8 of the 1907 Hague Convention 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 account of in the cyber context. This especially holds true for a "public, internationally and openly accessible network such as the Internet". Hence, 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."[36]

It must be noted that the HPCR Manual does not distinguish between mere communications on the one hand and the transmissions of cyber weapons on the other hand. 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 effectively exercise the control necessary for an effective interference 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 destination. Therefore, the mere fact that military communications, including cyber attacks, have been transmitted via the cyber infrastructure of a neutral State might not be considered a violation of that State's neutral obligations.

It is admitted that despite of the attractiveness of the HPCR Manual's approach for both belligerents and neutral States it is far from clear whether such a far-reaching adaptation of Article 8 Hague V to cyber operations conducted for military purposes will ultimately be accepted as reflecting 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), does not necessarily provide sufficient evidence that any cyber operation, including the transmission of cyber weapons, through neutral cyber infrastructure does not constitute a violation of neutrality. On the one hand, there is no unclassified information that the respective cyber operations did amount to cyber attacks and that they had been routed through neutral cyber infrastructure. The DDoS attacks against Georgia, according to the position taken here, do not qualify as cyber attacks and can therefore not be assimilated to the transit of "munitions of war" under Article 2 of Hague Convention V. On the other hand, the U.S. DoD Cyberspace Policy Report seems

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

36 HPCR Manual (*supra* note 10), Rule 167(b).

to justify the conclusion that the U.S. government is prepared to consider every "malicious cyber activity" as in violation of the law of neutrality irrespective of whether they have been launched from or merely transmitted through "computers or other infrastructure located in an neutral third country".[37]

Hence, it may be held that the use of neutral cyber communications by a belligerent does not constitute a violation of neutrality even though it serves military purposes. However, it is less clear whether this finding also holds true if the cyber operation in question qualifies as a 'malicious cyber activity' or as a 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.

4. OBLIGATIONS OF NEUTRAL STATES

The law of neutrality, in view of its object and purpose[38], poses obligations not only upon the belligerents but also on neutral States. Leaving aside the duty of impartiality[39], these obligations may be divided into three categories: (1) prohibition to allow or to tolerate the exercise of belligerent rights; (2) obligation to terminate (and probably to prevent) a violation of neutrality by a belligerent; and (3) obligation to tolerate the enforcement of the law of neutrality by the aggrieved belligerent.

A. Prohibition of Tolerating the Exercise of Belligerent Rights

According to Article 5 of the 1907 Hague Convention 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 is prohibited to allow or to tolerate the exercise of belligerent rights from the cyber infrastructure located within its territory or that is located outside its territory, provided that the neutral State exercises exclusive control over it.[40]

It may be noted that the different interpretations of Article 8 of Hague V may have far-reaching consequences. According to the approach taken in the HPCR Manual[41], a malicious cyber activity routed through neutral cyber infrastructure that is a component of, e.g., the Internet, would not constitute a prohibited exercise of belligerent rights. Hence, a neutral State allowing or tolerating such an activity would not violate its obligations under the law of neutrality. If the HPCR approach is not considered as reflecting 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 allowing or tolerating 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.

37 *Supra* note 21, at 8.
38 *Supra* note 17 and accompanying text.
39 Article 9 of the 1907 Hague Convention and Article 9 of the 1907 Hague Convention XIII provide that "every measure of restriction or prohibition taken by a neutral Power […] must be impartially applied by it to both belligerents." Hence, restrictions on military communications via its cyber infrastructure must be applied impartially by the neutral State. See also San Remo Manual (*supra* note 8), para. 19.
40 *Supra* 3. A.
41 *Supra* note 36.

Contrary to a position taken in the literature[42], the use of the term "allow" in the traditional rule presupposes knowledge by the organs of the neutral State. That will be the case if the organs have detected a malicious cyber activity/cyber attack or if they have been informed, e.g. by the other belligerent and in a sufficiently credible manner, that the activity has originated from, or has been transmitted through, the respective neutral State's cyber infrastructure. However, 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 a considerably high speed so that *ex-post-facto* knowledge can hardly suffice to justify a claim of a violation of the law of neutrality. And even if one were prepared to consider constructive (as opposed to actual) knowledge as sufficient for a violation of the said obligation that would not result in noticeable changes. Constructive knowledge means that the organs of a neutral State should have known of the malicious activity. Again, in most cases constructive knowledge would not necessarily result in a violation of neutral obligations.

This 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 whether such an obligation exists. Of course, the San Remo Manual, *inter alia*, 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."[43] It is, however, not likely that especially those States that defend the freedom of Internet communications will agree that the obligation to monitor territory and certain sea areas applies equally to the cyber infrastructure located in their territory.

B. 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 its neutrality by one of the belligerents.[44] This obligation is part of contemporary customary international law.[45]

The obligation to enforce its neutral status against violations by the belligerents is not absolute in character but it 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 within its territory.[46] The applicable standard is, thus, not objective but rather subjective. Everything will depend on the means and capabilities factually available to the respective neutral State. It needs to be emphasized that, subject to feasibility, the duty to enforce its neutral status entails an obligation to use all means necessary to effectively terminate an unlawful exercise of belligerent rights. This may include the use of force. The belligerent against whom such enforcement measures are applied may not consider them as a hostile act, i.e., it is obliged to tolerate them.[47]

42 Kastenberg (*supra* note 19), at 57.
43 San Remo Manual (*supra* note 8), para. 15.
44 *Ibid*., paras. 18 and 22; HPCR Manual (*supra* note 10), Rule 168(a). See also Articles 42 and 47 of the 1923 Hague Rules (*supra* note 27).
45 San Remo Manual (*supra* note 8), para. 22; HPCR Manual (*supra* note 10), Rule 168(a); NWP 1-14M (*supra* note 4), para. 7.3; German Manual (*supra* note 7), para. 1109.
46 *Ibid*.
47 Article 10 of the 1907 Hague Convention V; HPCR Manual (supra note 10), Rule 169; Hague Rules (*supra* note 27), Article 48.

The obligation to terminate an ongoing (!) violation of neutrality presupposes – actual or constructive – knowledge on part of the organs of the neutral State.[48] 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 from the neutral State to take measures against the respective belligerent because the cyber operation triggering the duty to terminate will no longer continue.

Obviously, such a limitation to ongoing (malicious) cyber activities is considered by some authors to be insufficient. They therefore claim that a neutral State is also obliged to take all feasible measures to prevent an exercise of belligerent rights, i.e., before it occurs.[49] 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.[50] 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 territory and national airspace. It is far from clear whether States are willing to accept it when it comes to the use of their cyber infrastructure because that would imply an obligation to continuously monitor cyber activities originating from or transiting through their cyber infrastructure. Moreover, the identification of the malicious nature of data packages transiting through a network would in most cases be most difficult, if not impossible.

Therefore, there are good reasons for rejecting a (prospective) duty of prevention. If at all, such an obligation would only exist with regard to activities within neutral territory that could be assimilated to those covered by Article 8 of the 1907 Hague Convention XIII.[51] 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 that is 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 (jurisdiction).

C. Consequences of Non-Compliance by Neutral States

Admittedly, during the international armed conflicts since the end of the Second World War neutral States have regularly not complied with their obligations under the law of neutrality.[52] They either openly or clandestinely assisted one party to an international armed conflict to the detriment of the other belligerent. However, already the fact that some neutral governments have tried to conceal their 'unneutral service' is sufficient evidence that they considered themselves bound by the law of neutrality. And even those governments that openly supported one side of an international armed conflict took pains in justifying their conduct. Eventually they were in

48 *Supra* 4. A.

49 Kastenberg (*supra* note 19), at 56 *et seq*.

50 San Remo Manual (*supra* note 8), para. 15; HPCR Manual (*supra* note 10), Rule 168(a); NWP 1-14M (*supra* note 4), para. 7.3.

51 "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."

52 See Heintschel von Heinegg (*supra* note 12), at 556 *et seq*.

a comfortable position in view of the fact that the aggrieved belligerent was unable to react to their non-compliance with neutral obligations.

The law of neutrality provides that if a neutral State fails to terminate (or prevent) an exercise of belligerent rights or another violation of neutrality by one belligerent, the other belligerent is entitled to take the measures necessary to terminate the violation.[53] 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 (or prevent) a violation of its neutral status by the enemy. This right is a specific form of a counter-measure, i.e., a measure that would be unlawful were it not taken in response to a violation of international obligations by the target State.[54] Its object and purpose is (1) to induce the neutral State to comply with its obligations; and (2) to enable the aggrieved belligerent to preserve its security interests. Hence, not every violation of the neutral status by one belligerent justifies a resort to counter-measures 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 imply a military advantage over the enemy. The right to respond to the violation is then exclusively reserved to the neutral State. Moreover, the exercise of the right is probably subject to a *de minimis* exception.

Moreover, the aggrieved belligerent is not entitled to immediately resort to the exercise of counter-measures. For instance, 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."[55] An immediate response by the aggrieved belligerent is lawful only, if

- the violation constitutes a serious and immediate threat to the security of that belligerent;
- there is no feasible and timely alternative; and
- the enforcement measure taken is strictly necessary to respond to the threat posed by the violation.[56]

The aggrieved belligerent's right to enforce the law of neutrality certainly applies to cyberspace if a malicious cyber activity originates from within the territory of a neutral State.[57] The U.S. DoD seems to be prepared to take such enforcement measures if it is possible to determine that a neutral State is aware of a malicious cyber activity within neutral territory. The DoD will take account of the following aspects:

- "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

53 NWP 1-14M (*supra* note 4), para. 7.3; San Remo Manual (*supra* note 8), para. 22; HPCR Manual (*supra* note 10), Rule 168(b).
54 International Law Commission, *Responsibility of States for Internationally Wrongful Acts*, Articles 22, 49-54, U.N. Doc. A/56/10.
55 San Remo Manual (*supra* note 8), para. 22.
56 *Ibid*. See also HPCR Manual (*supra* note 10), Rule 168(b).
57 See the Cyberspace Policy Report (*supra* note 21), at 8.

- The appropriate course of action for the U.S. Government to address potential issues of third-party sovereignty depending upon the particular circumstance."[58]

This is a clear restatement of the rules of the law of neutrality and it gives sufficient evidence of the DoD's willingness to apply those rules to conduct in cyberspace.

5. CONCLUSIONS

It has been shown that the traditional law of neutrality is, in principle, applicable to cyberspace, especially to belligerent cyber operations that violate the status of neutral States because they qualify as an exercise of belligerent rights within neutral territory. The special characteristics of cyberspace do not as such pose an obstacle to such application. However, there certainly 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 their potentially disastrous effects on critical infrastructure there is a high probability that belligerent States will take measures against neutral States and their respective cyber infrastructure, including the use of (kinetic) force if they must assume that vital security interests are at stake. Such measures have the potential of jeopardizing the essential object and purpose of the law of neutrality, i.e., preventing an escalation of an international armed conflict. The U.S. government has taken first steps that are most helpful in the identification of the applicable rules of international law and their interpretation in the light of the challenges brought about by the specific characteristics of cyberspace. The U.S. government should continue those efforts and other governments should closely cooperate with the U.S. government with a view to arriving at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cyber security due diligence.[59]

58 *Ibid*.
59 U.S. President, *International Strategy for Cyberspace*, at 10 (May 2011).