# Baltic Yearbook of International Law

## Volume 14, 2014


BRILL
NIJHOFF

LEIDEN | BOSTON

## Contents

### Symposium "Low Intensity Cyber Operations – The International Legal Regime", organized by the NATO Cooperative Cyber Defense Centre of Excellence and the Faculty of Law of the University of Tartu, 17–18 February 2014



### Articles

# Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations?

*Karine Bannelier-Christakis**

**Contents**



## 1. Introduction

The multiplication of cyber operations which target States' administrations, the economic sector and vital infrastructure[1] is today widely seen as one "the most pressing and potentially dangerous"[2] threats for national and international security.[3] While these operations do not reach the threshold of an "armed attack" within the meaning of *jus contra bellum*, their damaging impact raises nonetheless pressing questions about the duties of States in this field and the ability of international law to deal with this new threat. For many observers, there is no need to develop new norms. According for example to the *White House International Strategy for Cyberspace* "[t]he

* Associate Professor of International Law, Centre for International Security and European Studies, University of Grenoble-Alps.

1 This increase is well illustrated for example by the annual *Internet Security Threat Report*. The 2013 Report highlights that "[i]f 2011 was the year of the breach, then 2013 can best be described as the Year of the Mega Breach" with over 552 million identities breached. Symantec Corporation, *Internet Security Threat Report,* 2014, Volume 19, p. 5.

2 General S. Abrial 'NATO Builds its Cyberdefenses', *The New York Times*, 27 February 2011.

3 *See* NATO, *Strategic Concept for the Defence and Security of The Members of the North Atlantic Treaty Organisation*, Adopted by Heads of State and Government in Lisbon, Lisbon 19 November 2010, para. 12.



*Baltic Yearbook of International Law, Volume 14, 2014, ISBN: 978-90-04-29112-6, pp. 23–39.*

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 behaviour – in time of peace and conflict – also apply in cyberspace."[4] Among these customary and "long standing international norms", the principle of due diligence holds a special place. Indeed, this principle obliges States to protect foreign States and their citizens against illegal acts committed by non-state actors on their territories or under their jurisdiction or control.

The objective of this paper is to evaluate the relevance of this old principle – as it was conceived long before the invention of the "cyber sphere", at a time when space was finite and obvious. How can this old wine fit into the new bottles of ubiquitous and dematerialised low-intensity cyber operations that do not quite reach the level of an armed attack?

I will firstly briefly outline the meaning of due diligence in international law (2). I will then introduce what I call the "cyber diligence" concept, which concerns the applicability of the due diligence principle in cyberspace (3) and discuss the relevance in this field of the fundamental element of knowledge (4). I will then turn to a series of specific and tough questions concerning the parameters of this "cyber diligence" obligation and the need to find a right balance between the obligation to protect States and citizens against damaging cyber operations and the obligation to respect other international rules such as, for example, the right to privacy (5). Having this in mind I will thus examine successively the existence of an eventual obligation to enact legislation and domestic norms to forbid and condemn cyber acts against others States and the existence of an obligation of all States to secure their own cyber infrastructure (6). I will conclude with a discussion on the content of the duty to react in relation to cyber acts which are conducted against another State (7).

In order to inform the concept of "cyber diligence", I will use the whole panoply of international Law, from general international law concerning the rights and duties of States, to more specific branches, such as the obligation of prevention in international environmental law or the theory of "positive obligations" of states in international human rights law.

## 2. Due Diligence as a Principle of General International Law

The principle of due diligence is derived from the principle of sovereignty of States. According to Max Huber in the *Island of Palmas* arbitration:

> Territorial sovereignty … involves the exclusive right to display the activities of a State. This right has as corollary a duty: the obligation to protect within the terri-

4 The White House, *International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World* (Washington 2011), p. 9.

> tory the rights of other States, in particular their right to integrity and inviolability in peace and in war.[5]

This duty of due diligence has since then been reaffirmed and developed in many cases. Among them, the most famous one is undoubtedly the *Corfu Channel* case in which the International Court of Justice (ICJ) famously said that "every State [has the] obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States".[6]

Today, everybody agrees that the *dictum* of the Court expresses a general principle of international law. It is also accepted that the duty of diligence goes beyond the territory of States and covers "all activities which take place under the jurisdiction or control" of States[7] whereas these activities are conducted by the State itself or by others entities private as public.[8]

---

5 *Island of Palmas* case (*Netherlands* v. *USA*) 4 April 1928, *Reports of International Arbitral Awards*, United Nations, Vol. II, p. 839. *See also* the *Spanish Zone* case where Max Huber stated that "[l]a responsabilité pour les évènements de nature à affecter le droit international, se passant dans un territoire déterminé, va de pair avec le droit d'exercer à l'exclusion d'autres Etats les prérogatives de la souveraineté", in *Réclamations Britanniques dans la zone espagnole du Maroc (Grande-Bretagne* c. *Espagne)*, *ibid.*, p. 649.

6 ICJ, *Corfu Channel* case, Judgment of 9 April 1949, *ICJ Reports* 1949, p. 22.

7 According to the Tallinn Manual, "[t]his rule [due diligence] also applies with regards to acts contrary to international law launched from cyber infrastructure that is under the exclusive control of a government. It refers to situations where the infrastructure is located outside the respective State's territory, but that State nevertheless exercises exclusive control over it. Examples include a military installation in a foreign country subject to exclusive sending State control pursuant to a basing agreement, sovereign platforms on the high seas or in international airspace, or diplomatic premises", in M. N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyberwarfare* (NATO Cooperative Cyber Defence Centre of Excellence, Cambridge, Cambridge University Press, 2013) para. 8, pp. 27–28. *See also* the statement of the ICJ in the *Pulp Mills* case according to which, diligence was due in respect to "all activities which simply take place under the jurisdiction and control of each party", ICJ, *Pulp Mills on the River Uruguay (Argentina* v. *Uruguay),* Judgment of 20 April 2010, *ICJ Reports* 2010, para. 197.

8 According to J. G. Lammers, "States are not only obliged to prevent violations of those rights committed by their organs but are also obliged to prevent inroads on the interests protected by those rights by the conduct of individuals or private entities from within their territories", in J. G. Lammers, *Pollution of International Watercourses* (The Hague, Nijhoff, 1984) p. 527 cited in International Law Commission, 'Second Report on the Law of the Non-Navigational Uses of International Watercourses, by Stephen C. McCaffrey, Special Rapporteur', 2:1 *Yearbook of the International Law Commission* (1986) p. 116, footnote 191.

The "rights" to which the Court refers to are *all* unlawful acts that produce detrimental effects on another State.[9] Nonetheless, while the occurrence of a damage to a third State is a necessary condition in order to engage the responsibility of the State for violation of the due diligence principle, it is not a sufficient one. Due diligence is an obligation of conduct, not an obligation of result.[10] According to S. Heathcote, this means that States should "deploy their best efforts to achieve [the] desired outcome ... even if that outcome need not be ensured".[11] However, the term "best efforts"[12] could give the impression that we are in the borderline between a normative and a merely political obligation.[13] It could thus be better to declare that States have the obligation to "employ all available means" or "to take all available measures", or to "do all that could be reasonably expected of them".[14]

As the ICJ said in 2007 in the *Genocide* case:

---

9 According to the *Tallinn Manual*, "[t]his obligation applies not only to criminals acts harmful to others States, but also, for example, to activities that inflict serious damage, or have the potential to inflict such damage, on persons and objects protected by the territorial sovereignty of the target State", in Schmitt, *supra* note 7, p. 26 para. 3. And the *Manual* adds that "this rule covers all acts that are unlawful and have detrimental effects on another State" (p. 27, para. 5).

10 "It is an obligation of conduct, not an obligation of result" stated the International Law Commission in its commentary of Article 7 concerning the due diligence that watercourse States need to exercise. International Law Commission, 'Draft Articles on the Law of the Non-Navigational Uses of International Watercourse sand Commentaries thereto and Resolution on Transboundary Confined Groundwater', *Report of the International Law Commission on the Work of its Forty-sixth Session*, 1994. In a similar way *see also Pulp Mills*, *supra* note 7, paras. 186–187.

11 S. Heathcote, 'State Omissions and Due Diligence: Aspects of Fault, Damage and Contribution to Injury in the Law of State Responsibility', in K. Bannelier, T. Christakis and S. Heathcote (*eds.*), *The ICJ and the Evolution of International Law: The Enduring Impact of the Corfu Channel Case* (London-New York, Routledge 2012) p. 308.

12 According to the International Law Commission, "[o]bligations of prevention are usually construed as best efforts obligations, requiring States to take all reasonable or necessary measures to prevent a given event from occurring, but without warranting that the event will not occur", International Law Commission, 'Draft articles on Responsibility of States for Internationally Wrongful Acts with commentaries'*, Report of the International Law Commission on the work of its fifty-third session*, 2001, p. 62.

13 *See* R. P. Mazzeschi, *Responsabilité de l'Etat pour violation des obligations positives relatives aux droits de l'Homme*, 333 *Collected Courses of the Hague Academy of International Law* (2008) p. 284.

14 As the European Court of Human Rights decided in the *Osman* case, "it is sufficient … to show that the authorities did not do all that could be reasonably expected of them to avoid a real and immediate risk to life of which they have or ought to have knowledge", European Court of Human Rights, *Osman* v. *United Kingdom*, Judgment of 28 October 1998, ECHR 1998-VIII, para. 116.

> [I]t is clear that the obligation in question is one of conduct and not one of result, in the sense that a State cannot be under an obligation to succeed, whatever the circumstances, in preventing the commission of genocide: the obligation of States parties is rather to employ all means reasonably available to them, so as to prevent genocide so far as possible. A State does not incur responsibility simply because the desired result is not achieved; responsibility is however incurred if the State manifestly failed to take all measures to prevent genocide which were within its power, and which might have contributed to preventing the genocide. In this area the notion of "due diligence", which calls for an assessment *in concreto*, is of critical importance.[15]

## 3. From Due Diligence to "Cyber Diligence"

As a general principle of international law the duty of diligence applies to all activities including of course cyber activities. According to Rule 5 of the *Tallinn Manual*, "[a] State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely affect other States."[16]

This duty of cyber diligence applies to all cyber activities whether they are of "high" or "low" intensity, and whether these cyber operations are launched from the territory of a State or just *routed* by the territory of a State. Indeed, despite the hesitation of some experts,[17] there is no legal reason to consider that transit States do not have a duty of diligence and thus could escape their own obligations in this respect. For example, if a State knows that a terrorist group is about to cross its territory to attack a third State, the duty to act and to prevent exists. The same applies

15 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina* v. *Serbia and Montenegro)*, Judgment of 26 February 2007, *ICJ Reports* 2007, para. 430.

16 Schmitt, *supra* note 7, Rule 5: "Control of cyber infrastructure", p. 26. *See also* H. H. Koh (Legal Advisor of the US Department of State) for which "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict. The physical infrastructure that supports the internet and cyber activities is generally located in sovereign territory and subject to the jurisdiction of the territorial State. Because of the interconnected, interoperable nature of cyberspace, operations targeting networked information infrastructures in one country may create effects in another country. Whenever a State contemplates conducting activities in cyberspace, the sovereignty of other States needs to be considered", USCYBERCOM Inter-Agency Legal Conference Ft. Meade, MD, 18 September, 2012. According also to M. N. Schmitt and L. Vihul, "the principle of sovereignty protects cyber infrastructure on a State's territory irrespective of whether it is government owned or private", in M. N. Schmitt and L. Vihul, 'The International Law of Attribution During Proxy "Wars" in Cyberspace', 1 *Fletcher Security Review* (2014) p. 4.

17 The *Tallinn Manual* underlines that no consensus among experts of the *Tallinn Manual* was reached "whether this rule applies to State through which cyber operations are routed.", in Schmitt, *supra* note 7, p. 28, para. 12.

in principle to illegal cyber-attacks. This being said, we should not underestimate the extraordinary challenges created by the nature of the operations and a messy cyberspace. In several cases it would be impossible to prove that there was knowledge of these actions in a transit State. And, even if such knowledge were to exist, the available time for an appropriate reaction is of critical importance. Indeed, as the ICJ recognised in the *Corfu Channel* case the availability of enough time in order to notify third States and to react is very important in order to assess if a State failed in relation to its due diligence obligation.[18] With regard to the rapidity of transit in cyberspace, it is therefore unlikely that any State of transit could be held accountable for violating the due diligence principle. On the other hand if a cyber-attack is launched using public or private computers located in the transit State and the latter had or ought to have had the knowledge and the means to avert the situation the outcome could be different.

## 4. Knowledge as a Decisive Element of the Due Diligence Principle

Knowledge is the first decisive element of due diligence. In the *Hostages* case, the ICJ engaged Iran's responsibility after concluding that "the Iranian authorities (b) *were fully aware* … of the urgent need for action on their part; (c) had the means at their disposa1 to perform their obligations; (d) completely failed to comply with these obligations".[19]

States cannot nonetheless have an absolute knowledge of all things happening on their territory. This is why in *Corfu* the ICJ stated that "it cannot be concluded from the mere fact of the control exercised by a State over its territory and waters that that State necessarily knew, or ought to have known" what was happening.[20]

In a similar way the European Court of Human Rights observed, in its famous *Osman* v. *United Kingdom* case concerning the right to life, that:

> [f]or the Court, and bearing in mind the difficulties involved in policing modern societies, the unpredictability of human conduct and the operational choices which must be made in terms of priorities and resources, *such an obligation must be interpreted in a way which does not impose an impossible or disproportionate burden on the authorities*.[21]

18 As the ICJ determined, "Albania's obligation to notify shipping of the existence of mines in her waters depends on her having obtained knowledge of that fact in sufficient time before October 22; and the duty of the Albanian coastal authorities to warn the British ships depends on the time that elapsed between the moment that these ships were reported and the moment of the first explosion", *Corfu Channel* case, *supra* note 6, p. 22.

19 ICJ, *United States Diplomatic and Consular Staff in Teheran (United States of America* v. *Iran)*, Judgment of 24 May 1980, *ICJ Reports* 1980, para. 68.

20 *Corfu Channel* case, *supra* note 6, p. 18.

21 *Osman* v. *United Kingdom*, *supra* note 14, para. 116. Accordingly, not every claimed risk to life can entail for the authorities a requirement to take operational measures to prevent that risk from materialising.

### *4.1. Knowledge and the Standard of Proof*

The first problem is what will then be the standard of proof in order to show that a State *knew* that hostile cyber operations were taking place on its territory? Due to the fact that States exercise exclusive territorial control within their frontiers, this proof could become a real *probatio diabolica* for victims. Indeed, the victims of a breach of international law could be unable to furnish direct proof of facts to demonstrate the existence of knowledge.[22] In order to avoid this the ICJ said in the *Corfu Channel* judgment that it should "be allowed a more liberal recourse to interferences of fact and circumstantial evidence … The proof may be drawn from inferences of fact, provided that they leave no room for reasonable doubt."[23]

In that case the ICJ found that one of the indications of Albanian's knowledge of events was the fact that Albania, after the reported events affecting the United Kingdom, did not inquire into the event nor proceeded to judicial investigation.[24]

### *4.2. The Dilemma between Knowledge and Constructive Knowledge*

This second problem is even trickier. Although it is uncontroversial that the duty of diligence applies automatically in cases where States have actual knowledge of cyber acts in question[25] one should ask whether it should also be applicable in cases of constructive knowledge, when States o*ught* to have known about a specific situation.

The *Tallinn Manual* has hesitated handing down a conclusion on this point stating that the International Group of Experts "could not achieve consensus as whether this rule applies if the respective State has only constructive ('should have known') knowledge ... if it fails to use due care".[26]

---

22 As the ICJ observed, "the fact of this exclusive territorial control exercised by a State within its frontiers has a bearing upon the methods of proof available to establish the knowledge of that State as to such events. By reason of this exclusive control, the other State, the victim of a breach of international law, is often unable to furnish direct proof of facts giving rise to responsibility", in *Corfu Channel* case, *supra* note 6, p. 18.

23 *Ibid.* (emphasis added). The Court adds also that "[t]his indirect evidence is admitted in all systems of law, and its use is recognized by international decisions. It must be regarded as of special weight when it is based on a series of facts linked together and leading logically to a single conclusion", *ibid.* On the question of the standard of proof used by the ICJ *see* K. Del Mar, 'The International Court of Justice and standards of proof', in Bannelier, Christakis and Heathcote, *supra* note 11, pp. 98–123.

24 As the ICJ stated, "[a]nother indication of the Albanian Government's knowledge consists in the fact that that Government *did not notify* the presence of mines in its waters, at the moment when it must have known this ... further, whereas the Greek Government immediately appointed a Commission to inquire into the events of October 22, the *Albanian Government took no decision of such a nature, nor did it proceed to the judicial investigation* incumbent, in such a case, on the territorial sovereign", in *Corfu Channel* case, *supra* note 6, pp. 19–20 (emphasis added).

25 *See for example* the *Tallinn Manual* according to which, "[t]he Rule applies if the State has actual knowledge of the acts in question", in Schmitt, *supra* note 7, p. 28, para. 10.

26 *Ibid.*, p. 28, para. 11.

Here again the case law of the ICJ seems useful. In *Corfu Channel* the Court said that a State on whose territory an act contrary to international law has occurred "may be called upon to give an explanation [and] *cannot evade such a request by limiting itself to a reply that it is ignorant of the circumstances of the act and of its authors.* The State may, up to a certain point, be bound to supply particulars of the use made by it of the means of information and inquiry at its disposal."[27]

This conclusion is directly linked to the duties related to the exclusive control exercised by States over their territory. In a similar way the European Court of Human Rights (ECtHR) or the Human Rights Committee constantly accept the idea of constructive knowledge as part of the "positive obligations" of States in the field of Human Rights. As the ECHR said in *Osman* v. *United Kingdom*:

> [W]here there is an allegation that the authorities have violated their positive obligation … , it must be established … that the authorities *knew or ought to have known* at the time of the existence of a real and immediate risk to the life of an identified individual or individuals from the criminal acts of a third party and that they failed to take measures within the scope of their powers which, judged reasonably, might have been expected to avoid that risk.[28]

### *4.3. Knowledge and Monitoring*

This brings us to the nature of measures that States should adopt in order to be in a position to 'know' if illegal cyber acts which are hostile toward third States take place on their territory. Does due diligence imply an obligation for States to monitor cyber activities on their territory? The answer to this question is positive because, as it will be seen later, due diligence implies not only an obligation *to react* but also *to prevent*. Vigilance and monitoring thus go hand in hand.

In the *Pulp Mills* case the ICJ held that due diligence implied "the exercise of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators, to safeguard the rights of the other party".[29]

The recent French *White Book on Defence* also presents monitoring as a cornerstone in the fight against cyber activities which are dangerous for the security of States.[30]

---

27 *Corfu Channel* case, *supra* note 6, p. 18 (emphasis added).

28 *Osman* v. *United Kingdom*, *supra* note 14, p. 116. *See also* ECtHR, *Paul and Audrey Edwards* v. *United Kingdom*, Judgment of 14 March 2002, 2 *Reports of Judgments and Decisions*, 2002, para. 55.

29 *Pulp Mills*, *supra* note 7, para. 197.

30 According to the French *White Paper on Defence and National Security*, "[t]he new importance of cyber-threats calls for developing our intelligence activity and the corresponding technical expertise in this area. This effort should allow us to identify the origin of attacks, assess the offensive capabilities of potential adversaries and in this way counter their action. Identification and offensive action capabilities are essential

But what a slippery slope! Could due diligence become a kind of Trojan horse in order to erode civil liberties starting with the right to privacy and the respect of correspondence? Electronic surveillance programs such as *Prism* have given rise to heated debate and have been considered by some as being of an "almost-Orwellian" nature.[31] It should be recalled, nonetheless, that the duty of due diligence can only authorise acts compatible with international law. In the *Genocide* case the ICJ warned that "it is clear that every State may only act within the limits permitted by international law".[32] The ECtHR and other human rights treaty bodies also constantly emphasise that the police must exercise "their powers to control and prevent crime in a manner which fully respects the due process and other guarantees which legitimately place restraints on the scope of their action to investigate crime and bring offenders to justice".[33]

It is thus clear that the "knew or ought to have known" criterion cannot legitimise violations of international human rights or other rules. The resolution *The Right to Privacy in the Digital Age*, adopted by the UN General Assembly in December 2013, is a good example of what States should respect in this domain. This resolution invites States:

> (*a*) To respect and protect the right to privacy, including in the context of digital communication; (*b*) To take measures to put an end to violations of those rights and to create the conditions to prevent such violations, including by ensuring that relevant national legislation complies with their obligations under international human rights law; (*c*) To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law.[34]

This question of monitoring is directly linked not only to the requirement of "knowledge", but also to the more general question of the duty for States to prevent an act occurring which is contrary to the rights of others States.

---

to implementing a possible and appropriate response to such attacks", *French White Paper: Defence and National Security*, 2013, p. 71. *See also* French Network and Information Security Agency (ANSSI), *Information Systems Defence and Security: France's Strategy*, 2011, p. 15.

31 As US Judge Richard Leon concluded about the "bulk collection of Americans' telephone records by the NSA" in S. Ackerman and D. Roberts, 'NSA phone surveillance program likely unconstitutional, federal judge rules', *The Guardian*, 16 December 2013.

32 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina* v. *Serbia and Montenegro)*, *supra* note 15, para. 430.

33 *Osman* v. *United Kingdom*, *supra* note 14, para. 116.

34 A/Res/68/167, *The Right to Privacy in the Digital Age*, 18 December 2013.

## 5. Cyber Diligence as an Obligation of Prevention

The obligation of prevention as a corollary of due diligence is well routed in international jurisprudence. In the *Alabama* case, the Tribunal found that:

> the British government failed to use due diligence in the performance of its neutral obligations; and especially that it omitted, notwithstanding the warnings and official representations made by the diplomatic agents of the United States during the construction of the said number '290', to take in due time any effective *measures of prevention*, and that those orders which it did give at last, for the detention of the vessel, were issued so late that their execution was not practicable.[35]

In the same way the United States-Mexico Claims Commissions in the *Youmans* case found that State must satisfy its duty of prevention in order to fulfil its due diligence obligation and that Mexico failed its due diligence obligation by not preventing the attack resulting in the death of American citizens.[36] It is thus not surprising that in the *Corfu Channel* case, the ICJ concluded that "nothing was attempted by the Albanian authorities to *prevent* the disaster. These grave omissions involve the international responsibility of Albania."[37] And about 60 years later in the *Armed Activities on the Territory of The Congo*, the ICJ held Uganda responsible "for any lack of vigilance in *preventing* violations of Human Rights and International Humanitarian Law by other actors present in the occupied territory, including rebel groups acting on their own account".[38] Thus if the existence of a duty of prevention is in no way doubted, the exact content of this duty needs to be discussed.

### *5.1. A Duty of Prevention based on the Criterion of Reasonableness*

What kind of measures of prevention do States need to take? The international protection of human rights gives us some very interesting insights in this field, especially with the development of the so-called "positive obligations". Indeed, the international

35 *Alabama Claims of the United States of America against Great Britain*, Award rendered on 14 September 1872 by the tribunal of arbitration established by Article I of the Treaty of Washington of 8 May 1871, *United Nations, Reports of International Arbitral Awards*, Vol. XXIX, p. 130 (emphasis added).

36 *Thomas H. Youmans (USA)* v. *United Mexican State*, 23 November 1926, United Nations, *Reports of International Arbitral Awards*, Vol. 4, para. 12, p. 115. *See* on this question S. B. Crandall, 'Principles of International Law Applied by the Spanish Treaty Claims Commission', 4:4 *American Journal of International Law* (1910) pp. 806–822. *See also* R. P. Barnidge, 'State's Due Diligence Obligations with regard to International Non-State Terrorist Organizations Post-11 September 2001: The Heavy Burden that States must Bear', 16 *Irish Studies in International Affairs* (2005) pp. 106–110.

37 *Corfu Channel* case, *supra* note 6, p. 23.

38 ICJ, *Armed Activities on the Territory of the Congo (Democratic Republic of the Congo* v. *Uganda)*, Judgment of 19 December 2005, *ICJ Reports* 2005, para. 179.

protection of human rights involves not only duties of abstention, but also *obligations to act* in order to prevent any violations of human rights by non-state actors.

The European Court of Human Rights, the Human Rights Committee and several other treaty bodies have constantly proclaimed the idea that if a State "knew or ought to have known" of the situation and failed to "take appropriate measures" or "to exercise due diligence to prevent" or "to do all that could be reasonably expected of it" therein exists a violation of international law.[39]

While all these bodies accept that this "duty to act and prevent" should not create an impossible burden on authorities, they all focus on the criterion of "reasonableness" which is decisive here. In the case *Kiliç* v. *Turkey* for example, the European Court of Human Rights held Turkey responsible for the violation of the right to life for the resulting murder of a journalist that the authorities failed to protect despite numerous death threats. The Court said that the authorities failed to act even though "[a] wide range of preventive measures were available which would have assisted in minimizing the risk to Kemal Kılıç's life and which would *not have involved an impractical* diversion of resources".[40]

On the contrary, in the Ärzte für das Leben v. *Austria* judgment of 1991, concerning the complaint of a non-governmental organisation to the Court about the State's failure to protect demonstrators (during a protest against abortion) against the action of counter-demonstrators, the ECtHR found that there was no violation of Article 13 since it "clearly appears that the Austrian authorities did not fail to take reasonable and appropriate measures" as "a hundred policemen were sent to the scene to separate the participants from their opponents and avert the danger of direct attacks".[41]

---

39 In the *Lopez Ostra* v. *Spain* case the European Court of Human Rights held for the first time that a failure by the State to control industrial pollution by private actors was a violation of Article 8 because there was sufficiently serious interference with the applicants' enjoyment on their home and private life. The Court spoke about "a positive duty on the State – to take reasonable and appropriate measures to secure the applicant's rights", European Court of Human Rights, *Lopez Ostra* v. *Spain*, Judgment of 9 December 1994, ECHR A303-C, para. 51. The Human Rights Committee also clearly recognises that [t]he legal obligation under article 2, paragraph 1 [of the ICCPR], is both negative and positive in nature. … There may be circumstances in which a failure to ensure Covenant rights as required by article 2 would give rise to violations by States parties of those rights, as a result of States parties' permitting or failing to take appropriate measures or to exercise due diligence to prevent, punish, investigate or redress the harm caused by such acts by private persons or entities", Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, 26/05/2004, paras. 6, 8.

40 European Court of Human Rights, *Kiliç* v. *Turkey*, Judgment of 28 March 2000, ECHR Rec. 2000-III, para. 76.

41 European Court of Human Rights, Ärzte *für das Leben* v. *Austria,* Judgment of 21 June 1988, ECHR Rec. 1988, paras. 38–39.

In other fields of International Law also this criterion of "reasonableness" appears in relation with the principle of due diligence. The criterion of "reasonableness" was clearly affirmed by the ICJ in the *Genocide* case,[42] but also in several arbitrations concerning the protection of aliens. In the case *A. H. Francis* v. *United Mexican States*, the British-Mexican Claim Commission found that despite the murder of a British citizen, the Mexican State had not failed in adopting "reasonable measures" of prevention because "[t]here is no direct evidence whatever of negligence on the part of the authorities, and the British Agent did not even suggest any specific measures that they should have taken. In no country in the world can isolated crimes of this nature be prevented".[43] This case also shows that the notion of reasonableness is often cited in relation with the concept of negligence when assessing the respect by States of their diligence obligation. In the old *Alabama* arbitration, for instance, the arbitral tribunal underlined that "notwithstanding the warnings" the United Kingdom did not take the effective measures of prevention and thus found that there was "negligence"[44] on the part of that State.

### *5.2. An Obligation to Enact Preventive Domestic Normative Measures?*

Does the "duty to prevent" include a duty to enact legislation and domestic normative measures? If we accept that such an autonomous obligation exists, we might slip from the kingdom of obligations of "conduct" to the one of obligations of "result". In the field of human rights, several treaty bodies insist on the existence on an obligation "to adopt laws for the effective protection of the rights and freedoms"[45] proclaimed by human rights treaties. The responsibility of States has often been engaged by human rights treaty bodies for failure to adopt necessary domestic measures.[46]

We maybe find ourselves at the limits of the comparison between the theory of positive obligations in human rights law and the general international law due diligence principle. Indeed one could argue that the "positive obligation" to take legislative, judicial and administrative measures in the field of human rights derives directly from the commitments of States under human rights treaties – such as Article 2(2) of the International Covenant on Civil and Political Rights.[47] But could such an obligation exist in the field of cyber diligence without a specific treaty?

---

42 *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina* v. *Serbia and Montenegro)*, *supra* note 15, para. 430.

43 *A. H. Francis (Great Britain)* v. *United Mexican States,* Decision No. 15, 15 February 1930, United Nations, *Report of International Arbitral Awards,* vol. 5, p. 100, para. 5,

44 *Alabama Claims of the United States of America against Great Britain*, *supra* note 35, p. 131.

45 CIDH, *Castillo-Petruzzi et al.* v. *Peru*, Judgment of 30 May 1999, Series C no. 52, para. 202, al. *e* (emphasis added).

46 *See for example Lopez Ostra* v. *Spain*, supra note 39, para. 51.

47 According to Article 2(2), "[w]here not already provided for by existing legislative or other measures, each State Party to the present Covenant undertakes to take the necessary steps, in accordance with its constitutional processes and with the provisions of the

It goes without saying that enacting legislative measures in order to prevent and punish cyber acts contrary to the right of other States is *one of the best ways* to implement the "due diligence" obligation. Measures of prevention of cyber-attacks will require almost inevitably such legislative measures and many States have already expressed their concern to adapt their legislative framework in this field.[48] But since due diligence is an obligation of conduct States do have *the choice* of the best measures to take depending of the circumstances.

Consequently we come to one of the limits of due diligence in relation to low-intensity cyber operations. If we want to "upgrade" State's obligations concerning cyber diligence, in order to impose *specific* and *detailed* obligations on States the adoption of an international treaty would probably be necessary. One of the best examples of this is, of course, the Convention on Cybercrime adopted by the Council of Europe in 2001.[49] This Convention provides for the harmonisation of the domestic criminal substantive law elements of offences in the area of cybercrime and also provides for the domestic criminal procedural law powers necessary for the investigation and prosecution of such offences.[50] These measures are very important but only a multilateral instrument can introduce such specific obligations.

Whatever the conclusion – whether or not there is an obligation for State to enact domestic law in order to prevent cyber activities contrary to the rights of others States, it is interesting to note that, according to the tribunal in the *Alabama* case, States cannot claim the insufficiency of its legal means to justify its failure in due

present Covenant, to adopt such legislative or other measures as may be necessary to give effect to the rights recognized in the present Covenant.", International Covenant on Civil and Political Rights, UN General Assembly, 19 December 1966, *UN Treaty Series*, Vol. 999, 1-14668. According to the Human Rights Committee, "[i]t follows that, unless Covenant rights are already protected by their domestic laws or practices, States Parties are required on ratification to make such changes to domestic laws and practices as are necessary to ensure their conformity with the Covenant. Where there are inconsistencies between domestic law and the Covenant, article 2 requires that the domestic law or practice be changed to meet the standards imposed by the Covenant's substantive guarantees", Human Rights Committee, *General comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, 26/05/2004, para. 13.

48 *See for example* French Network and Information Security Agency (ANSSI), *supra* note 30*,* pp. 17–18.

49 Council of Europe, Convention on Cybercrime, 23 November 2001, *European Treaty Series* – No. 185.

50 *See* especially Articles 2 to 8 which oblige State Parties to adopt legislative and other measures to establish as criminal offences: the illegal access to a computer (Article 2); the illegal interception of computer data (Article 3); data interference (Article. 4); system interference (Article 5); misuse of devices (Article 6); computer-related forgery (Article 7); computer-related fraud (Articlet. 8), *ibid.*

diligence.[51] This means that in any situation a State cannot escape its obligation by invoking the failure of its legislative *apparatus.*

## 6. An Obligation to Protect Cyber Infrastructure?

Related to the question of adoption of an adequate legislation stands the question of whether a State has an obligation to protect its cyber infrastructure against any interference or misuse.

According to the *US International Strategy for Cyberspace*, cybersecurity due diligence implies that "States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse".[52] In the same vein the French *Livre Blanc sur la Défense* focused on the need of securing vital infrastructure.[53]

In March 2010, the UN General Assembly adopted also a very interesting resolution entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures".[54] Annexed to this Resolution the UN General Assembly adopted a "Voluntary self-assessment tool for national efforts to protect critical information infrastructures calls States to determine and assess the protection of their vital infrastructure".

But whatever the interest of these incentives, the question is to know whether due diligence includes an obligation for States to protect their own cyber infrastructures. The answer should be that due diligence requires States to take "all appropriate measures" in order to avoid cyber-attacks. If a State totally failed to secure its own cyber infrastructure, a failure which then authorised hostile groups to use this infrastructure as a weapon, the responsibility of the State could be engaged. As the ICJ judged in the *Genocide* case, "violation of the obligation to prevent results from omission".[55]

But unlike the adoption of legislation, States are not equal when they try to protect their infrastructures. In the *Alabama* case the US said that due diligence "is a diligence proportioned to the magnitude of the subject and to the dignity and

51 *Alabama Claims of the United States of America against Great Britain*, *supra* note 35, p. 131.

52 The White House, *supra* note 4, p. 10.

53 *Livre Blanc: Défense et Sécurité Nationale*, 2013, p. 106. *See also* French Network and Information Security Agency (ANSSI), *supra* note 30, p. 17.

54 A/Res/64/211, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures*, 17 March 2010. This resolution, which follows resolutions adopted since 2000 on the misuse of information technologies and the creation of a global culture of cybersecurity, affirms that the securing of cyber infrastructure is under the responsibility of Governments. *See also* subsequent resolutions in this field until A/Res/68/243, *Developments in the field of information and telecommunications in the context of international security*, 27 December 2003.

55 ICJ, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina* v. *Serbia and Montenegro)*, *supra* note 15, para. 432.

strengthen of the power which is to exercise it".[56] The requirement of securing cyber infrastructure should be proportionate to the cyber capacities/technologies of that State. The proportionality of the requirement is directly linked with the reasonableness criterion of the principle of prevention described above.[57]

However, it should be underlined that failure to adopt legislation or to protect cyber infrastructure will not immediately constitute a breach of due diligence.[58] Indeed, the occurrence of harm is necessary to engage State responsibility for lack of due diligence. As stated by the International Law Commission in its Article 14(3) on State Responsibility, "[t]he breach of an international obligation requiring a State to prevent a given event occurs when the event occurs".[59]

This leads us to a last series of questions concerning the obligation of reaction which, undoubtedly, is the most well-known element of the duty of diligence.

## 7. An Obligation to React

It is well established that, under the due diligence principle, States have an obligation to notify and warn the potential victims of the cyber-attacks. This obligation to notify has been clearly stated, for example, by the ICJ in the *Corfu Channel* case.[60]

---

56 J. B. Moore, *International Arbitrations to which the United States has been a Party*, Vol.1, pp. 572–573.The weakness of some States to exercise their responsibility in this field raises of course many questions. Even if due diligence does not imply right now an obligation to cooperate with the least developed countries, it is clear that if States want to secure their own infrastructure against misuse, they could greatly benefit in helping developing countries to upgrade their own capacity-building. In this sense Resolution 64/211 is an interesting one by "*[s]tressing* the need for enhanced efforts to close the digital divide in order to achieve universal access to information and communications technologies and to protect critical information infrastructures by facilitating the transfer of information technology and capacity-building to developing countries, especially the least developed countries, in the areas of cybersecurity best practices and training", A/Res/64/211, *supra* note 54.

57 *See supra* section 5.1.

58 According to R. Ago, "[t]o our knowledge, decisions of international tribunals have never affirmed, even indirectly or incidentally, that failure to adopt measures to prevent the occurrence of a possible event sufficed in itself – i.e., without the actual occurrence of such an event – to constitute a breach of the obligation incumbent on the State", in R. Ago, 'Seventh report in State Responsibility', I:1 *ILC Yearbook* (1978) para. 11, p. 34. *See* in this respect Heathcote, *supra* note 11, p. 311.

59 International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations, 2001.

60 According to the Court: "the only conclusion to be drawn would be that a general *notification* to the shipping of all States before the time of the explosions would have been difficult, perhaps even impossible. But this would certainly not have prevented the Albanian authorities from taking, as they should have done, all necessary steps immediately to *warn* ships near the danger zone, more especially those that were approaching that zone", ICJ, *Corfu Channel* case, *supra* note 6, pp. 22–23.

But the obligation to react is not just an obligation to notify. As the *Tallinn Manual* has rightly recognised, in case of injury to another State the State where the cyber operation takes place will be obliged to use all means at its disposal "to *terminate* the activity".[61] If the obligation of termination of the illegal activity is not controversial in itself, the implementation and the exact scope of this obligation could raise some questions. Indeed, in order to stop a cyber-attack, States can use different tools that have, in some cases, more or less serious negative effects on third-parties countries and civilians. There is in this field an obligation for States to assess the necessity of their reaction and its proportionality.[62]

Of course, as always, this test is not an easy one. But it is nonetheless necessary in order to avoid states acting in a disproportionate manner or using the principle of due diligence as a mere pretext in order to follow a hidden agenda. During the evaluation of the proportionality and the reasonableness of the reaction, one should take once again into account the fact that these measures do not violate international law and especially human rights law. As stated by the *US International Strategy for the Cyber Space*, freedom of expression, intellectual property and rights to privacy are among these fundamental freedoms that State should protect.[63]

Moreover States have an obligation to investigate and punish the authors of such acts. Once again we can recall that in the *Corfu Channel* case the ICJ found that an indication of Albanian's knowledge of what was occurring was the fact that Albania, after the events affecting the United Kingdom took place, did not inquire into the event nor proceeded to judicial investigation "incumbent, in such a case, on the territorial sovereign".[64]

The case law of the human rights treaty bodies is also very clear in this field. Due diligence includes a duty to investigate. As the Inter-American Court of Human Rights famously proclaimed in the *Velásquez Rodríguez* case:

> The State is obligated to investigate every situation involving a violation of the rights protected by the Convention. If the State apparatus acts in such a way that the violation goes unpunished. … the State has failed to comply with its duty. … In certain circumstances, it may be difficult to investigate acts that violate individual

61 Schmitt, *supra* note 7, p. 28, para. 9.

62 As the *Tallinn Manual* states, "[t]he nature, scale and scope of the (potential) harm to both state must be assess to determine whether this remedial measure is required. The test in such circumstances is one of reasonableness", *ibid.,* p. 27, para. 4.

63 The White House, *supra* note 4, pp. 23–24.

64 As the Court pronounced, "[a]nother indication of the Albanian Government's knowledge consists in the fact that that Government *did not notify* the presence of mines in its waters, at the moment when it must have known this … further, whereas the Greek Government immediately appointed a Commission to inquire into the events of October 22, the *Albanian Government took no decision of such a nature, nor did it proceed to the judicial investigation* incumbent, in such a case, on the territorial sovereign", *Corfu Channel* case, *supra* note 6, pp. 19–20.

> rights. The duty to investigate, like the duty to prevent, is not breached merely because the investigation does not produce a satisfactory result. Nevertheless, it must be undertaken in a serious manner and not as a mere formality preordained to be ineffective … Where the acts of private parties that violate the Convention are not seriously investigated, those parties are aided in a sense by the government, thereby making the State responsible on the international plan.[65]

By obliging States to adopt criminal sanctions that are "effective, proportionate and dissuasive"[66] including the possibility of prison sentences, the European Convention on Cybercrime could be a reference in this field.

## 8. Conclusion: Towards a Cooperative Cyber Diligence?

Due diligence is not only an obligation of reaction; it is also an obligation of knowledge and of prevention. This does not mean that this obligation is of "high intensity". Its nature as an obligation of means/conduct based on the criterion of "reasonableness" means that States do not carry a too heavy burden. The difficulty to apprehend activities in cyberspace makes its application even more complicated.

The due diligence principle derived from general international law is certainly a useful starting point in order to organise the fight against States that could be tempted to turn their territory into a kind of "cyber haven" or "cyber paradise" for cyber criminals or even cyber terrorists. It is also important that this principle does not authorise States to turn, in the name of their duty to protect the rights of other States, their territory into a kind of "cyber hell" destroying the freedom of speech and the right to privacy. But, as useful and balanced as this principle might be, the ubiquity of cyber operations makes it difficult for States to implement the principle alone. The development of a notion of "cooperative cyber diligence" will probably be necessary in the future to harmonise the efforts of the international community and to ensure the effectiveness of the principle. But if we want to go further and to "upgrade" this cyber diligence obligation we should think about the adoption in the future of a universal instrument on cybersecurity proposing a right balance between these competitive interests.

65 Inter-American Court of Human Rights, *Velásquez Rodríguez* v. *Honduras,* Judgment of 29 July 1988, Cn° 4, paras. 176–177. *See also* European Court of Human Rights, *Mc Cann and others* v. *United Kingdom*, Judgment of 25 September 1995, ECRH, A324, para. 161 and Human Rights Committee, *General Comment No. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, CCPR/C/21/Rev.1/Add.13, 26/05/2004, par. 15.

66 Convention on Cybercrime, *supra* note 49, Article 13.