Human Rights Obligations of the Territorial State in the Cyberspace of Areas Outside Its Effective Control

Antal Berkes[*]

The absence of control of a territorial state over part of its physical territory is closely associated with online human rights violations, on the one hand, and the state's restricted (but not necessarily absent) control over the cyberspace, on the other. Notwithstanding the lack of its effective territorial control, the territorial state continues to be entitled to exercise its sovereignty over both territory and cyberspace. The consequence of sovereignty in international human rights law is the territorial state's presumed jurisdiction over its entire national territory. The article claims that the territorial state, while lacking the effective means to control its cyberspace fully as it does in the government-controlled areas, has continuing jurisdiction, and consequently obligations, to protect human rights online from wrongful acts that originate, occur or have effect in the area outside its effective control. Treaty monitoring bodies have recommended various positive measures that any territorial state is required to take while seeking to restore its 'internet sovereignty' in the separatist region, depending on the means in its power that are feasible in the particular situation.

Keywords: international human rights law, due diligence, cyberspace, effective control, *Ilaşcu* case

1. Introduction

Various contemporary territorial conflicts have resulted in areas falling outside the effective control of the sovereign state (territorial state) – such as Transnistria (1992), Nagorno-Karabakh (1988–94), South Ossetia (1991–92, 2008) and Abkhazia (1992–93), Crimea (2014) and the separatist areas in Eastern Ukraine (2014 to date) – or vast territories controlled by extremist terrorist groups in the Middle East, such as the Islamic State (2014 to date).[1] The state's lack of effective control over part of its territory raises multiple challenges for international law, which is traditionally based on the duties of the state that is presumed to have exclusive control over its sovereign territory.[2] Once the territorial state loses effective control over part of its territory – for various reasons, such as an armed conflict or consent given by the state to have its territory administered by an another subject of international law[3] – various norms of international law that bind the

[*] University of Pretoria, Post-Doctoral Fellow in the SARChI Professorship on International Constitutional Law (Professor Erika de Wet); Visiting scholar, Manchester International Law Centre, University of Manchester; antal.berkes@manchester.ac.uk (comments welcome). I thank the anonymous reviewers and the editorial team of the *Israel Law Review* for their most helpful comments.

[1] The article will not focus on other areas outside the effective control of the territorial state such as Northern Cyprus or Western Sahara, where there are no reported human rights violations in the cyberspace.

[2] ECtHR, *Assanidze v Georgia*, App no 71503/01, 8 April 2004, para 139; Gérard Kreijen, *State Failure, Sovereignty and Effectiveness: Legal Lessons from the Decolonization of Sub-Saharan Africa* (Martinus Nijhoff 2004) 204.

[3] The major precedents are international territorial administrations and leases of territory: see Markus Benzing, 'International Administration of Territories' (2010) *Max Planck Encyclopedia of Public International Law*; Yaël Ronen, 'Territory, Lease' (2008) *Max Planck Encyclopedia of Public International Law*. Two precedents where international territorial administrations performed all state functions in a territory under their control are

territorial state become ineffective. While each of those territorial situations gives rise to different legal regimes (such as the law of international armed conflict, the law of non-international armed conflict, the territorial lease agreement), a common element is an apparent legal *lacuna* in conventional human rights obligations of the international law subject that controls the territory. Furthermore, the actors controlling the area may be other states or even non-state actors (such as armed opposition groups, de facto regimes, international organisations), which may not be addressees of international law. Instead of the notion of 'ungoverned spaces', widely used in the literature,[4] it is more accurate to recognise that various actors – which are often states other than the territorial state and non-state actors – exercise effective control over the territory.

This means that often several states control the same territory (such as through a multinational operation) or that the conduct of a non-state actor in directly controlling the territory is attributed to an outside state. Therefore, the above-mentioned legal *lacuna* can be filled by new, or newly interpreted rules applied to the subjects that are active in the area: solutions proposed include the human rights obligations of the subject controlling the territory under the de facto control theory,[5] the acquired human rights doctrine,[6] and the concurrent obligations of various actors (states, non-state actors) exercising powers in the given area.[7] Furthermore, as this article will emphasise, even the territorial state has residual obligations under international human rights law (IHRL).

East Timor (governed by the United Nations Transitional Administration in East Timor, 1999–2002) and Kosovo (governed by the civilian mission, the United Nations Interim Administration Mission in Kosovo from 2008, significantly reduced following the declaration of independence by the Kosovo authorities). A contemporary precedent for leased territory is the Bay of Guantánamo under Cuban sovereignty but under US control: Agreement for the Lease to the United States of Lands in Cuba for Coaling and Naval Stations, signed at Havana, 16 February 1903, and at Washington, 23 February 1903, entered into force 23 February 1903, Charles I Bevans, *Treaties and Other International Agreements of the United States of America*, Department of State, vol 6, 1113–15, art III.

[4] Nicholas Tsagourias, 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts' (2016) 21 *Journal of Conflict and Security Law* 455; Anne L Clunan and Harold A Trinkunas (eds), *Ungoverned Spaces: Alternatives to State Authority in an Era of Softened Sovereignty* (Stanford Security Studies 2010); Steven Boraz and others, *Ungoverned Territories: Understanding and Reducing Terrorism Risks* (NBN 2007); Robert D Lamb, *Ungoverned Areas and Threats from Safe Havens: Final Report of the Ungoverned Areas Project* (Office of the Under Secretary of Defense for Policy (OUSD(P)) 2008).

[5] Michael Schoiswohl, 'De Facto Regimes and Human Rights Obligations: The Twilight Zone of Public International Law' (2001) 6 *Austrian Review of International and European La*w 45, 78–79; Daragh Murray, *Human Rights Obligations of Non-State Armed Groups* (Hart 2016) 126–28; Anthony Cullen and Steven Wheatley, 'The Human Rights of Individuals in De Facto Regimes under the European Convention on Human Rights' (2013) 13 *Human Rights Law Review* 691, 717–23.

[6] According to this theory, any subject undertaking effective control over the area is bound by the international human rights obligations of the territorial sovereign. This theory is confirmed in Human Rights Committee, General Comment No 26: Continuity of Obligations (8 December 1997), UN Doc CCPR/C/21/Rev.1/Add.8/Rev.1, para 4; International Criminal Tribunal for the former Yugoslavia (ICTY), *Prosecutor v Mucić*, Judgment, IT-96-21-A, Appeals Chamber, 20 February 2001, para 111.

[7] eg, Samantha Besson, 'Concurrent Responsibilities under the European Convention on Human Rights: The Concurrence of Human Rights Jurisdictions, Duties and Responsibilities' in Anne van Aaken and Iulia Motoc (eds), *The European Convention on Human Rights and General International Law* (Oxford University Press 2018). See also the recommendations of some Charter-based human rights mechanisms: UNGA, Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Mission to Israel and the Occupied Palestinian Territory (17 June 2012), UN Doc A/HRC/20/17/Add.2 (Human Rights Council, Mission to Israel), paras 9–13, 97–118 (concurrent obligations of various actors); UNGA, Human Rights Council, Report on the Human Rights Situation in Ukraine,

These areas are characterised by massive or repetitive human rights violations.[8] In fact, the protection of human rights in these areas is a far more complicated issue than is the case in government-controlled areas. The reasons for the apparent lack of clarity in the legal regime are various. First, human rights treaties impose obligations only on states;[9] second, they do not foresee a lack of effective control of the state over part of its territory; and, third, the obligations can hardly be enforced against other subjects that are de facto controlling the territory.

Furthermore, these areas are characterised by major human rights violations not only in the physical space, but also in cyberspace.[10] Freedom of expression, privacy, freedom of opinion, due process and human dignity, in particular, have been restricted online by actors which control the territory. Such actors have recourse to practices that restrict human rights online through censorship, the threat and manipulation of online media, undue blocking of access to certain websites or the internet as a whole, and dissemination of racial hatred and terrorist propaganda.[11]

Territorial states have had difficulties in preventing, repressing and redressing these wrongful acts. Notwithstanding these deficiencies, IHRL obliges the territorial state to take all measures within its power to protect human rights in the area outside its effective control.[12] The European Court of Human Rights (ECtHR), treaty monitoring bodies and organisations based on the UN Charter[13] have identified certain positive obligations that territorial states are required to take vis-à-vis persons situated in the area.[14] Specifically in the online context, those recommendations provide the basis for identifying various measures that any territorial state is required

16 May–15 August 2017 (15 September 2017), UN Doc A/HRC/36/CRP.2 (Human Rights Council, Ukraine 2017), paras 182–84.

[8] Council of Europe Parliamentary Assembly (CoE PA), 'Areas where the European Convention on Human Rights Cannot be Implemented', Doc 9730, 11 March 2003, paras 1, 6.

[9] The exception is the possibility of having international organisations as signatories: eg, Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (entered into force 1 August 2014) CETS 210, art 75(1); Convention on the Rights of Persons with Disabilities (entered into force 3 May 2008) 2515 UNTS 3, art 42.

[10] CoE PA, Resolution 2141(2017), 'Attacks against Journalists and Media Freedom in Europe', 24 January 2017, para 12; CoE PA, 'Attacks against Journalists and Media Freedom in Europe', Doc 14229, 9 January 2017, Explanatory Memorandum, para 82; European Parliament, 'Media Freedom Trends 2017: Eastern Partnership Countries, 3 May 2017, http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/603897/EPRS_BRI(2017)603897_EN.pdf; UN Human Rights Committee, Concluding Observations: Russian Federation (28 April 2015), UN Doc CCPR/C/RUS/CO/7, para 23(b); Human Rights Council, Situation of Human Rights in the Temporarily Occupied Autonomous Republic of Crimea and the City of Sevastopol (Ukraine) (25 September 2017), UN Doc A/HRC/36/CRP.3, paras 154–61; Office of the UN High Commissioner for Human Rights (UN OHCHR), Report on the Human Rights Situation in Ukraine, 15 July 2014 (19 September 2014), UN Doc A/HRC/27/75, 161–62 para 152; Security Council, Report of the Independent International Commission of Inquiry on the Syrian Arab Republic (5 February 2015), UN Doc A/HRC/28/69, Annex II, paras 82, 259. References to media in the cited documents include a particular means of mass communication, that disseminated in cyberspace

[11] Section 2 in this article.

[12] Section 4 in this article.

[13] Charter of the United Nations (entered into force 24 October 1945) 1 UNTS XVI.

[14] Sections 4 and 5 in this article.

to strive to take with a view to restoring its 'internet sovereignty'[15] (control over cyberspace in the area outside its effective control). This article focuses accordingly on the territorial state's obligations in the context of cyberspace under IHRL. While other related topics – such as human rights obligations of non-state armed groups[16] and occupying states,[17] the duties of states in cyberspace,[18] and their responsibility for the cyber conduct of non-state actors[19] – have been researched extensively in recent years, nothing has been written on the substantive obligations of the territorial state in the cyberspace of an area out of governmental control. Through the example of the territorial state's obligations, the article also addresses extensively debated questions such as the applicability of sovereignty to cyberspace, the scope of application of IHRL[20] and of the due diligence standard in cyberspace.

The article claims that the territorial state, while lacking the effective means to fully control its cyberspace as it does in government-controlled areas, has continuing jurisdiction and positive obligations to protect human rights in cyberspace from wrongful acts that originate, occur or have effect in the part of its territory outside its effective control. The article proceeds as follows. The following section (Section 2) demonstrates the challenges that loss of territorial control by the state poses for human rights in cyberspace. It will show that the absence of control over the physical space is closely associated with online human rights violations, on the one hand, and the state's restricted (but not necessarily non-existent) control over the cyberspace, on the other. Section 3 confirms that notwithstanding the lack of its effective territorial control, the territorial state continues to be entitled to exercise its sovereignty over both the territory and the cyberspace. Section 4 discusses the logical consequence of sovereignty in IHRL, the territorial state's jurisdiction based on so-called due diligence, considered as a corollary duty of the rights arising from sovereignty. Section 5 applies the rules of IHRL to the obligations of the territorial

[15] In the same sense see Timothy S Wu, 'Cyberspace Sovereignty: The Internet and the International System Notes' (1996) 10 *Harvard Journal of Law and Technology* 647.

[16] eg, Andrew Clapham, *Human Rights Obligations of Non-State Actors* (Oxford University Press 2006) 271–316; Katharine Fortin, *The Accountability of Armed Groups under Human Rights Law* (Oxford University Press 2017) 240–84; Murray (n 5) 120–271.

[17] eg, Eyal Benvenisti, 'The Applicability of Human Rights Conventions to Israel and to the Occupied Territories' (1992) 26 *Israel Law Review* 24; Orna Ben-Naftali and Yuval Shany, 'Living in Denial: The Application of Human Rights in the Occupied Territories' (2004) 1 *Israel Law Review* 17; John Cerone, 'Human Dignity in the Line of Fire: The Application of International Human Rights Law during Armed Conflict, Occupation, and Peace Operations' (2006) 39 *Vanderbilt Journal of Transnational Law* 1447; Danio Campanelli, 'The Law of Military Occupation Put to the Test of Human Rights Law' (2008) 90 *International Review of the Red Cross* 653; Noam Lubell, 'Human Rights Obligations in Military Occupation' (2012) 94 *International Review of the Red Cross* 317.

[18] Karine Bannelier-Christakis, 'Cyber Diligence: A Low-Intensity Due Diligence Principle for Low-Intensity Cyber Operations' (2014) 14 *Baltic Yearbook of International Law* 23; Russell Buchan, 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm' (2016) 21 *Journal of Conflict and Security Law* 429; Gabor Rona and Lauren Aarons, 'State Responsibility to Respect, Protect and Fulfill Human Rights Obligations in Cyberspace' (2016) 8 *Journal of National Security Law and Policy* 503; Matthew J Sklerov, 'Solving the Dilemma of Sate Responses to Cyberattacks: A Justification for the Use of Active Defenses against States Who Neglect Their Duty to Prevent' (2009) 201 *Military Law Review* 1.

[19] Tsagourias (n 4).

[20] Rona and Aarons (n 18) 506–09.

state in the context of cyberspace in areas outside its effective control. The conclusions provide some recommendations for enhancing human rights compliance of the territorial states concerned within the positive law framework of IHRL.

2. CYBERSPACE IN AREAS OUTSIDE THE EFFECTIVE CONTROL OF THE TERRITORIAL STATE

'[Cyberspace] is a world that is both everywhere and nowhere, but it is not where bodies live'.[21] It is 'a "borderless" world – computer-based communications cut across territorial borders creating a new realm of human activity',[22] and its innovative nature seems to provoke new problems in law, especially in international law.

The term 'cyberspace' can be defined as '[a] world-wide virtual space, different from real space, with many sub-communities unevenly distributed using a technical environment – first of all the internet – in which citizens and organizations utilize information and communication technology for their social and commercial interactions'.[23]

In other words, it is a fictional space (rather than having a tangible nature) used to describe the phenomenon of electronic signals transiting through the infrastructure of information and communications technology (ICT). It follows from the above definition that cyberspace has three layers: a physical layer (switches, routers, servers and cables), a software layer (logical network), and a third layer consisting of data packets and electronics – the people actually on the network (cyber-persona layer).[24] Despite its virtual nature, cyberspace necessarily requires a physical architecture.[25]

'Cyber activity' is a process in which information technology systems (including, inter alia, telecommunications and computer systems) are the means of activity.[26] This article focuses on those cyber activities that carry the risk of restricting human rights. While there is no internationally accepted list of human rights that can be affected in cyberspace, certain rights are more relevant than others in the cyber context. In this regard, the Tallinn Manual, a non-binding expert commentary on the international law applicable to cyber operations, is of guidance as it

[21] John P Barlow, 'A Declaration of the Independence of Cyberspace', *Electronic Frontier Foundation*, 8 February 1996, https://www.eff.org/cyberspace-independence. Others attribute the phrase to Jon Carroll, columnist of the *San Francisco Chronicle*: see 'The Geography of Cyberspace', *The Atlantic Online*, 19 February 1998, http://www.theatlantic.com/past/docs/unbound/citation/wc980219.htm.

[22] Asian-African Legal Consultative Organization (AALCO), 'International Law in Cyberspace', prepared by the AALCO Secretariat, 56th Annual Session of AALCO, Nairobi, 1–5 May 2017, Doc AALCO/56/NAIROBI/2017/SD/S17, para 1.

[23] UNESCO, 'Internet Governance Glossary', https://en.unesco.org/glossaries/igg/groups/1.%20Internet%20governance%20general.

[24] Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Nicholas K Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar 2015) 15; US Department of the Navy/US Department of the Air Force, *Cyberspace Operations*, Joint Publication 3-12 (R), 5 February 2013, I.2–I.3.

[25] Patrick W Franzese, 'Sovereignty in Cyberspace: Can It Exist?' (2009) 64 *Air Force Law Review* 1, 33.

[26] See, *mutatis mutandis*, 'The Definition of Cybercrime', UNTERM (UN Terminology Database), https://unterm.un.org/UNTERM/portal/welcome.

reflects an objective restatement of the *lex lata* by a group of experts.[27] The Manual provides a non-exhaustive list of particularly important human rights in cyberspace, highlighting freedom of expression, privacy, freedom of opinion, and due process.[28] One can also add the right to access information as part of freedom of expression[29] and human dignity, because the latter can be violated by various forms of expression such as racial discrimination,[30] incitement to terrorism[31] and child pornography.[32] This non-exhaustive list of the most affected human rights in cyberspace constitutes the focus of this article.

Because the ubiquitous and widely available character of cyberspace allows the carrying out of harmful cyber activities from any physical location, at first sight there is no correlation between an area outside the effective control of the state and online human rights violations. However, as this section will demonstrate, the territorial state's lack of control over the physical area is closely associated with online human rights violations, on the one hand, and the state's restricted (but not necessarily non-existent) control over the cyberspace, on the other.

Recent territorial conflicts have resulted in areas being outside the effective control of the territorial state. Examples are Transnistria, Nagorno-Karabakh, South-Ossetia and Abkhazia, Crimea and the separatist areas in Eastern Ukraine, as well as vast territories controlled by extremist terrorist groups in the Middle East, such as the Islamic State. As mentioned above, these areas are characterised not only by human rights violations in the physical territory but also those committed online. The violations in cyberspace have been committed by various actors, especially non-state de facto authorities, an outside state controlling the area and/or the territorial state.

---

[27] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017) 2–3; International Law Commission (ILC), Second Report on the Protection of the Environment in relation to Armed Conflicts, submitted by Marie G Jacobsson, Special Rapporteur (28 May 2015), UN Doc A/CN.4/685, para 180.

[28] Schmitt, ibid 187 para 1. See also UNGA, Human Rights Council, Res 38/7, The Promotion, Protection and Enjoyment of Human Rights on the Internet (17 July 2018), UN Doc A/HRC/RES/38/7, para 8 (emphasising 'freedom of opinion and expression, freedom of association and privacy').

[29] eg, Universal Declaration of Human Rights (UDHR), UNGA Res 217A(III), 10 December 1948, UN Doc A/810 (1948), art 19; European Convention on Human Rights and Fundamental Freedoms (entered into force 3 September 1953) 213 UNTS 222 (ECHR), art 10(1); International Covenant on Civil and Political Rights (entered into force 23 March 1976) 999 UNTS 171 (ICCPR), art 19(2).

[30] International Convention on the Elimination of All Forms of Racial Discrimination (CERD) (entered into force 4 January 1969) 660 UNTS 195 (CERD), art 5(d)(viii).

[31] Council of Europe, Convention on the Prevention of Terrorism (entered into force 1 June 2007) CETS 196, art 5. The UN Special Rapporteur, while countering terrorism, held that this provision represents best practice in defining the proscription of incitement to terrorism: UNGA, Human Rights Council, Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, Australia: Study on Human Rights Compliance while Countering Terrorism (14 December 2006), UN Doc A/HRC/4/26/Add.3, para 26.

[32] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (entered into force 18 January 2002) 2171 UNTS 227, arts 1–2(c).

First, de facto authorities often force online media to terminate or self-censor their activities,[33] using threats and manipulation.[34] In the areas controlled by the Islamic State in Iraq and the Levant (ISIL), the organisation's militants murdered digital activists and bloggers;[35] internet access was subject to restrictive regulations;[36] and internet users had to increase their self-censorship in order to avoid criticising the militants or Islam in general.[37] Beyond the restriction of online media operating in the area, de facto authorities might block certain websites or media channels diffused from outside the area – a measure referred to generally as 'information blockade'.[38] By way of example, the de facto authorities in Transnistria blocked Moldovan channels[39] and a dozen news portals and websites with anti-government content,[40] and the 'Donetsk People's Republic' similarly shut down several internet-based media outlets.[41]

Second, outside states controlling an area as occupying powers are reported to have committed similar human rights violations. Censorship,[42] physical harassment of online journalists,[43] and information blockade have characterised recent occupations. During and following the Georgian-Russian war of 2008, Georgia and Russia mutually blocked Georgian and Russian internet sites and television channels.[44] In Crimea, the Russian authorities block Ukrainian

[33] See, eg, UN OHCHR, Report on the Human Rights Situation in Ukraine, 15 June 2014 (19 September 2014), UN Doc A/HRC/27/75, 110–11 para 232; Freedom House, 'Freedom in the World 2012: Nagorno-Karabakh', https://freedomhouse.org/report/freedom-world/2012/nagorno-karabakh; Freedom House, 'Freedom in the World 2016: Nagorno-Karabakh', https://freedomhouse.org/report/freedom-world/2016/nagorno-karabakh; Freedom House, 'Freedom in the World 2018: Abkhazia', https://freedomhouse.org/report/freedom-world/2018/abkhazia; Freedom House, 'Freedom in the World 2017: South Ossetia', https://freedomhouse.org/report/freedom-world/2017/south-ossetia.

[34] UN OHCHR, ibid 110–11 para 232 (the Donetsk region); UN OHCHR, Ukraine (15 July 2014) (n 10) 161–62 para 152 (the Donetsk region).

[35] Freedom House, 'Freedom on the Net 2016: Syria', https://freedomhouse.org/report/freedom-net/2016/syria.

[36] ibid; UNGA, Human Rights Council, 'Report of the Independent International Commission of Inquiry on the Syrian Arab Republic' (1 February 2018), UN Doc A/HRC/37/72, para 66. The Islamic State in Libya used the same technique: Freedom House, 'Freedom on the Net 2016: Libya', https://freedomhouse.org/report/freedom-net/2016/libya.

[37] Freedom House: Syria (n 35).

[38] eg, 'TV Says Ukraine Losing "Information War" in Donbass due to Underfunding', *BBC International Reports*, 28 March 2018.

[39] Freedom House, 'Freedom in the World 2016: Transnistria', https://freedomhouse.org/report/freedom-world/2016/transnistria.

[40] Freedom House, 'Freedom in the World 2014: Transnistria', https://freedomhouse.org/report/freedom-world/2014/transnistria; Promo-LEX, 'Freedom of Expression in the Transnistrian Region of the Republic of Moldova: 2016 Retrospective', 2017, 15, https://promolex.md/wp-content/uploads/2017/03/eng-Raport-EXPRIMARE-web_2017.pdf; US State Department, 'Moldova 2016 Human Rights Report', 17–18, https://www.state.gov/documents/organization/265662.pdf.

[41] UN OHCHR, Report on the Human Rights Situation in Ukraine, 16 May to 15 August 2015, para 70, https://www.ohchr.org/Documents/Countries/UA/11thOHCHRreportUkraine.pdf.

[42] UN OHCHR, Report on the Situation of Human Rights in the Temporarily Occupied Autonomous Republic of Crimea and the City of Sevastopol, Ukraine, 13 September 2017 to 30 June 2018, para 47, https://www.ohchr.org/Documents/Countries/UA/CrimeaThematicReport10Sept2018_EN.pdf.

[43] UN OHCHR, Ukraine (15 June 2014) (n 33) 122 para 300.

[44] Organization for Security and Co-operation in Europe (OSCE) Press Release, 'OSCE Media Freedom Representative Says Journalists Need Free and Safe Access to Georgia's South Ossetia and Abkhazia Regions', 22 September 2008, http://www.osce.org/fom/50101.

internet sites and force local web-based outlets to relocate to the Ukrainian government-controlled territories.[45]

Third, while addressing the territorial situation by military, intelligence or administrative means, even territorial states have restricted the online human rights of persons situated in the area outside their effective control. Invoking national security or the fight against terrorism, various territorial states have had recourse to extreme forms of information blockade, such as blocking websites without a proper investigation and a court decision,[46] or shutting down the internet in the area outside their control[47] or even nationwide.[48] The said measures unduly restrict online communication in a given area, whereas freedom of expression should apply 'regardless of frontiers'.[49]

While online human rights violations might be committed in normal circumstances in any state's government-controlled territory, the characteristic of the situations referred to above is the limited capacity of the territorial state to prevent, repress and redress those wrongful acts. In fact, the territorial states concerned have often reiterated their inability to implement their obligations with regard to human rights treaties[50] in general, and with regard to a treaty that specifically imposes obligations in respect of cyberspace, the Budapest Convention on Cybercrimes,[51] in particular. Once the state loses effective control over part of its territory, it loses its law enforcement capacity as well as physical access to victims and the actual authors

[45] Human Rights Committee, Concluding Observations: Russian Federation (n 10) para 23(b).

[46] While Ukrainian authorities asked the Ukrainian Internet Association for its assistance in limiting access in Ukraine to 24 internet resources registered outside Ukraine, the Association refused to block websites without a proper investigation and a court decision for each case: UN OHCHR, Report on the Human Rights Situation in Ukraine, 17 August 2014 (19 September 2014), UN Doc A/HRC/27/75, 209. Similarly, the Syrian government in 2012 blocked around 240 websites, including email services, social media, and streaming video: Olesya Tkacheva and others, *Internet Freedom and Political Space* (RAND Corporation 2013) 77–78.

[47] 'Iraq Telecom Ministry Orders ISPs: Kill the Internet in Five Provinces', *SMEX: Channeling Advocacy*, 16 June 2014, https://smex.org/iraq-telecom-ministry-orders-isps-kill-the-internet-in-five-provinces.

[48] 'Syria "Cut off from the Internet"', *BBC News*, 8 May 2013, https://www.bbc.co.uk/news/world-middle-east-22446041.

[49] UDHR (n 29) art 19; ECHR (n 29) art 10(1); ICCPR (n 29) art 19(2); Budapest Convention on Cybercrime (entered into force 1 July 2004) ETS 185, Preamble, para 9; UN World Summit on the Information Society, 'Declaration of Principles: Building the Information Society: A Global Challenge in the New Millennium', 12 December 2003, Doc WSIS-03/GENEVA/DOC/4-E, para 4; UNGA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet (29 June 2012), UN Doc A/HRC/RES/20/L.13, para 1.

[50] eg, Council of Europe Treaty Office, https://www.coe.int/en/web/conventions/full-list: Reservations and Declarations for Treaty No 005 (ECHR): Declarations of Azerbaijan (Declaration contained in the instrument of ratification deposited on 15 April 2002) and the Republic of Moldova (Declaration contained in the instrument of ratification deposited on 12 September 1997); Reservations and Declarations for Treaty No 009 (Protocol to the ECHR): Declarations of Azerbaijan (Declaration contained in the instrument of ratification deposited on 15 April 2002) and Georgia (Declaration contained in the instrument of ratification deposited on 7 June 2002); Reservations and Declarations for Treaty No 187 (Protocol 13 to the ECHR): Declarations of Georgia (Declaration contained in the instrument of ratification deposited on 22 May 2003) and the Republic of Moldova (Declaration contained in the instrument of ratification deposited on 18 October 2006). For the legal effect of those treaty declarations, see below (Section 4).

[51] See the Declaration of Azerbaijan, the Republic of Moldova and Ukraine to the Budapest Convention: Reservations and Declarations for Treaty No 185 (Convention on Cybercrime), status as at 29 June 2018, https://www.coe.int/en/web/conventions/full-list.

of the online human rights violations.[52] Furthermore, while cybercrimes and other online human rights violations can emanate from any place in the world, perpetrators are likely to find safe haven in areas outside the effective control of the territorial state where the latter cannot exercise its power of enforcement.[53] Some pro-Russian hacker groups, for example, perpetrate their attacks from Eastern Ukrainian areas outside the effective control of the Ukrainian government 'to bypass the territorial filters blocking IP addresses coming from Russia'.[54] With regard to cyberspace, with the loss of territorial control the territorial state necessarily loses control over the physical layers of the internet located in that area, but retains control over the physical layers located in the government-controlled area that might affect information transfer in the area outside its control. Therefore, as far as the territorial state might control cyber activities from the government-administered area, it might retain limited power with regard to online human rights violations committed in the area outside its effective control.

The existence of areas that escape the effective control of the territorial state not only facilitates massive human rights violations, but may constitute a threat to international peace and security.[55] The UN Security Council has expressed concern over the fact that ISIL used the internet and social media as promotional and recruitment tools for terrorist purposes[56] and for the online sale of Iraqi and Syrian antiquities.[57] Considering that the atrocities committed by ISIL may amount to crimes against humanity and possibly genocide,[58] the concept of 'responsibility to protect' has been applied.[59] Accordingly, the Security Council has underlined 'the need for Member States to act cooperatively to prevent terrorists from exploiting technology, communications and resources to incite support for terrorist acts'[60] and reiterated that 'the primary

[52] ICT for Peace Foundation and UN Counter-Terrorism Committee Executive Directorate (UNCTED), 'Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes: Strengthening Dialogue and Building Trust', 5, https://www.un.org/sc/ctc/wp-content/uploads/2016/12/Private-Sector-Engagement-in-Responding-to-the-Use-of-the-Internet-and-ICT-for-Terrorist-Purposes.pdf.

[53] Peter Margulies, 'Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights' (2017) 68 *Florida Law Review* 1045, 1088; Nadiya Kostyuk, 'Ukraine: A Cyber Safe Haven?' in Kenneth Geers (ed), *Cyber War in Perspective: Russian Aggression against Ukraine* (NATO CCD COE Publications 2015) 115.

[54] Marie Baezner, 'Cyber and Information Warfare in the Ukrainian Conflict', Center for Security Studies (CSS) Cyber Defense Project, ETH Zürich, 2017, 10.

[55] UNSC Res 2170 (15 August 2014), UN Doc S/RES/2170, preambular para 13; UNSC Res 2249 (20 November 2015), UN Doc S/RES/2249, preambular para 8.

[56] UNSC Res 2170, ibid, preambular para 13; UNSC Res 2395 (21 December 2017), UN Doc S/RES/2395, preambular para 27.

[57] UNSC Res 2199 (12 February 2015), UN Doc S/RES/2199, para 16.

[58] Human Rights Council, 'Commission of Inquiry on the Syrian Arab Republic, "They Came to Destroy": ISIS Crimes Against the Yazidis' (15 June 2016), UN Doc A/HRC/32/CRP.2.

[59] See the first pillar of the theory of 'Responsibility to Protect': UNGA Res 60/1(24 October 2005), UN Doc A/RES/60/1(2005), para 138, and the numerous resolutions of the Security Council confirming this obligation: eg, recently UNSC Res 2399 (30 January 2018), UN Doc S/RES/2399, preambular para 3; UNSC Res 2337 (19 January 2017), UN Doc S/RES/2337, preambular para 9. For a complete list see http://www.globalr2p.org/resources/335.

[60] UNSC Res 2170 (n 56) preambular para 13; UNSC Res 2395 (n 56) preambular para 27.

responsibility to protect its population lies' with the territorial state.[61] There is no reason to doubt that the primary responsibility of the territorial state to protect applies equally to atrocities committed online.[62]

Generally, most states find it challenging 'to exercise sovereignty over incidents of cyber-attacks, cyber-crimes as well as over cyber-related businesses within their territories'.[63] This applies *a fortiori* to territorial states, which have to face not only numerous online human rights violations in their territory, but also their lack of control over the physical space. This double difficulty of control, over the online and offline spaces, raises the question of how far cyberspace is subject to the territorial state's sovereignty in an area outside its effective control.

3. STATE SOVEREIGNTY IN CYBERSPACE

Because of its non-physical character, at first sight cyberspace hardly fits within the traditional principles of public international law such as sovereignty or territorial integrity,[64] also enshrined in the UN Charter.[65] A considerable group of libertarian scholars argue that cyberspace should not be regulated and subjected to state sovereignty, given its de-territorialised and, by definition, trans-boundary character.[66] However, the debate over whether cyberspace can or should be regulated 'has essentially waned and is largely a historical milestone', as noted by the International Law Commission (ILC).[67] Today it is widely recognised by states[68] and international law scholars[69]

[61] UNSC Res 2139 (22 February 2014), UN Doc S/RES/2139, paras 9, 12; UNSC Res 2254 (18 December 2015), UN Doc S/RES/2254, preambular para 4; UNSC Res 2258 (22 December 2015), UN Doc S/RES/2258, preambular para 8 ('the primary responsibility of the Syrian authorities to protect the population in Syria').

[62] Oren Gross, 'Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents' (2015) 48 *Cornell International Law Journal* 481, 491–93. Within the 'responsibility to protect' one could think of the crime of 'direct and public incitement to commit genocide' committed online: Convention on the Prevention and Punishment of the Crime of Genocide (entered into force 12 January 1951) 78 UNTS 277, art III(c).

[63] AALCO (n 22) para 4(1).

[64] Similar difficulties arise in private international law: Inter-American Judicial Committee, Annual Report of the Inter-American Judicial Committee to the General Assembly, OEA/Ser.Q/VI.34, CJI/doc.145/03, 29 August 2003, 164.

[65] Charter of the United Nations (n 13) art 2(1), 2(4).

[66] David R Johnson and David G Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stanford Law Review* 1367; Frank Easterbrook, 'Cyberspace and the Law of the Horse' (1996) *University of Chicago Legal Forum* 207; Antonio Segura-Serrano, 'Internet Regulation and the Role of International Law' (2006) 10 *Max Planck United Nations Yearbook of International Law* 191, 193–97.

[67] ILC, Report of the ILC on the Work of its 58th Session (1 May–9 June and 3 July–11 August 2006), UN Doc A/CN.4/SEA.A/2006/Add. 1 (Part 2), 2006(II) *Yearbook of the International Law Commission* 218 para 5.

[68] UN World Summit on Information Society (23 December 2003), UN Doc Wsis-03/GENEVA/DOC, para 49(a); AALCO, 'International Law in Cyberspace 2016', Doc AALCO/55/NEW DELHI/2016/SD/S17, paras 10 (People's Republic of China), 15 (Iran), 18 (South Africa), 20 (Pakistan), 21 (Democratic People's Republic of Korea). Not surprisingly, the territorial states concerned also emphasise their sovereign right to use the telecommunications networks in their territory: International Telecommunications Union, Final Acts of the Plenipotentiary Conference, Busan (South Korea), 2014, 522–23 (Declaration No 2, Georgia), 576–78 (Declaration No 76, Ukraine), http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.294.43.en.100.pdf.

[69] UNGA, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (24 June 2013), UN Doc A/68/98 (GGE Report 2013), para 20; UNGA,

that state sovereignty is applicable to cyberspace. Moreover, the number of international treaties governing cyberspace has increased.[70]

The regulation of de-territorialised telecommunications activities, however, is not a novel domain of international law: from the very beginning of the invention of wireless telegraphy, states undertook to exercise their sovereignty over radiotelegraphic communications in their territory.[71] Authors in the interwar period generally assumed that state control was necessary to regulate the international use of telecommunication techniques, and that a state incurs international responsibility for breaching the prohibition on interference in the internal affairs of other countries by propaganda hostile to another state through radio.[72] To the extent that cyberspace is also a wireless form of telecommunication, the same principles apply.[73]

The application of the principle of state sovereignty in cyberspace has its main rationale in the supreme authority of the state to regulate any cyber infrastructure located within its territory,[74] even though it may also exercise its sovereign prerogatives outside the territory.[75] The physical layer of cyberspace is therefore subject to the sovereignty of the territorial state, whereas the virtual domain of cyberspace does not fall within the sovereignty of a specific state.[76]

State sovereignty is closely related to state jurisdiction: the latter notion refers to the state's 'lawful power to act and hence to its power to decide whether and, if so, how to act, whether by legislative, executive, or judicial means'.[77] In other words, it is the competence of a state to regulate persons, objects, and conduct under its domestic law, within the limits set by

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (22 July 2015), UN Doc A/70/174 (GGE Report 2015), para 27.

[70] It is the Budapest Convention on Cybercrime (n 49), signed in 2001, that was the first international treaty to regulate conduct in the cyberspace; Additional Protocol to the Convention on Cybercrime, concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems (entered into force 1 March 2006) ETS 189; United Nations Convention on the Use of Electronic Communications in International Contracts (entered into force 1 March 2013) 2898 UNTS 1; League of Arab States, Arab Convention on Combating Information Technology Offences (entered into force February 2014), see the authentic Arab text and the ratification status at http://www.lasportal.org/ar/legalnetwork/Pages/agreements_details.aspx?RID=73 and the English translation at http://itlaw.wikia.com/wiki/Arab_Convention_on_Combating_Information_Technology_Offences; African Union Convention on Cyber Security and Personal Data Protection (adopted 27 June 2014, not yet in force) (2017) 56 ILM 166.

[71] International Radiotelegraph Convention (London, 5 July 1912), (1913) 10 *Treaty Series* 139–217, art 1; International Convention concerning the Use of Broadcasting in the Cause of Peace (entered into force 2 April 1938) 186 LNTS 301, art 1; Resolution on Radio-Telegraphic Communications (1927) *Annuaire de l'Institut de Droit International*, session de Lausanne, 287 and 342–43, para 1.

[72] Vernon Van Dyke, 'The Responsibility of States for International Propaganda' (1940) 34 *American Journal of International Law* 58, 58–59; Hersch Lauterpacht, 'Revolutionary Propaganda by Governments' (1927) 13 *Transactions Grotius Society* 143, 162; W Friedmann, 'The Growth of State Control over the Individual, and Its Effect upon the Rules of International State Responsibility' (1938) 19 *British Year Book of International Law* 118, 146–47.

[73] Schmitt (n 27) 26, 284–85, 312–35.

[74] ibid 11 para 1.

[75] ibid 60–71 (Rules 10–11).

[76] Tsagourias (n 24) 21, 27.

[77] Bernard H Oxman, 'Jurisdiction of States' (2007) *Max Planck Encyclopedia of Public International Law* para 1.

international law.[78] The term 'jurisdiction' also expresses 'the limits imposed under international law on the ability of a state to exercise prescriptive (or legislative) and enforcement jurisdiction' – that is, the circumstances in which the state is entitled to exercise its legal authority.[79] No state can perform enforcement functions in the territory of another state without the consent of the latter state.[80] This means that as long as the state is recognised by the international community as the sovereign of the area, it has jurisdiction over it, despite its lack of effective power to exercise its sovereignty in that area.[81]

Jurisdiction under general international law is primarily territorial – that is, the state enjoys full prescriptive, adjudicatory and enforcement jurisdiction over persons and objects situated in its internationally recognized territory, as well as over activity occurring there.[82] In the event of loss of effective territorial control, some authors consider the sovereignty of the territorial state as 'suspended'[83] or limited to '*nudum jus*'.[84] Because of its lack of effectiveness in the area, the state is indeed unable to exercise its enforcement jurisdiction, but is not necessarily unable to regulate and adjudicate activities occurring in the area.[85] It could be said that the laws and judicial decisions of the state concerning the area outside its control would have validity as far as the state can enforce them in the government-controlled area, or through international cooperation.[86] Consequently, the state, while unable to exercise its effective control over an

[78] Schmitt (n 27) 51.

[79] Olivier De Schutter and others, 'Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights' (2012) 34 *Human Rights Quarterly* 1084, 1102 para 3; Ralph Wilde, 'The Extraterritorial Application of International Human Rights Law on Civil and Political Rights' in Scott Sheeran and Sir Nigel Rodley (eds), *Routledge Handbook of International Human Rights Law* (Routledge 2013) 640.

[80] This rule can be derived from the territorial integrity and independence of states, as enshrined in art 2(4) of the UN Charter (n 13); *S.S. Lotus (France v Turkey)*, Judgment, (1927) PCIJ Rep (Ser A, No 10) 18–19; *Island of Palmas Case (United States v The Netherlands)* (1928) *Reports of International Arbitral Awards* (RIAA), Vol II, 829, 839.

[81] *Ottoman Debt Arbitration*, 18 April 1925, (1925) RIAA, Vol I, 555; *Fubini*, Decision No 201 of 12 December 1959, Italian-United States Conciliation Commission, (1959) RIAA, Vol. XIV, 429; *State of the Netherlands v Federal Reserve Bank of New York*, 201 F.2d 455 (2d Cir 1953), repr in (1953) 47(3) *American Journal of International Law* 498; *Armed Activities on the Territory of the Congo, Democratic Republic of the Congo v Uganda*, Judgment, [2005] ICJ Rep 306, Separate Opinion of Judge Kooijmans, 320–21 [57]; FE Oppenheimer, 'Governments and Authorities in Exile' (1942) 36 *American Journal of International Law* 568, 571.

[82] Schmitt (n 27) 52.

[83] Alexandros Yannis, 'The Concept of Suspended Sovereignty in International Law and Its Implications in International Politics' (2002) 13 *European Journal of International Law* 1037; Ronen (n 3) (the territorial state is 'divorced from jurisdiction').

[84] Georg Jellinek, *Die Lehre von Den Staatenverbindungen* (Hölder 1882) 54, 116; Valentina Azarova, 'Illegal Territoriality in International Law: The Interaction and Enforcement of the Law of Belligerent Occupation through Other Territorial Regimes' (PhD thesis, National University of Ireland Galway 2015) 94.

[85] On the state's lacking effectiveness in the territory, see in general Hans Kelsen, *General Theory of Law and State* (Russell & Russell 1961) 217–18.

[86] See the recognition of the jurisdiction of the ousted government in the law of belligerent occupation: 'Extraterritorial Enforcement Granted to Legislation of a Government-in-Exile' (1953) 53 *Columbia Law Review* 561; Yoram Dinstein, *The International Law of Belligerent Occupation* (Cambridge University Press 2009) 108–09.

area of its territory and thus enforce its laws there, can exercise its prescriptive and adjudicatory jurisdiction over the area.

The overwhelming majority of states do not contest the sovereignty and jurisdiction under general international law of the territorial states concerned. The Republic of Moldova, Azerbaijan, Georgia, Ukraine, the Republic of Cyprus, Iraq and Syria are all internationally recognised as sovereign over the disputed areas. Whether they have jurisdiction over the cyberspace in areas outside their effective control depends on the jurisdictional bases recognised in cyberspace.

Specifically in the context of online activities, the International Group of Experts in elaborating the Tallinn Manual 2.0 foresaw three major bases on which the state may exercise jurisdiction over cyber activities related to its territory. Rule 9 of the Manual allows the state to exercise jurisdiction over 'cyber infrastructure and persons engaged in cyber activities on its territory'; 'cyber activities originating in, or completed on, its territory'; and 'cyber activities having a substantial effect in its territory'.[87] As mentioned above, the Manual is intended to be an objective restatement of the *lex lata* and,[88] as it will be shown, the relevant rule on territorial jurisdiction reflects the existing (positive) international law as accepted by states.

The first of these three bases for jurisdiction relies on the fact that the physical presence of a person or an object in the territory of the state provides a sufficient basis for the exercise of jurisdiction by that state.[89] Since information and communication technologies require some physical infrastructure, states have jurisdiction over those objects and the persons engaged in cyber activities in their national territory.[90]

For example, it is recognised that states may exercise regulatory authority over the telecommunications or internet service providers that physically control the data in the territory of the state.[91] The territorial state's jurisdiction over cyber activities in areas outside its effective control is thus recognised when the persons engaging in cyber activities, or the cyber infrastructure (such as cable infrastructures, servers, computers, media production infrastructure or data storage facilities) are located in the area concerned.

The second basis for jurisdiction – cyber activities initiated or completed in the state's territory – relies on a principle of international law that has been recognised since the *Lotus* judgment, namely the subjective (activity originating in the state's territory) and objective (activity completed in the state's territory) territorial jurisdiction.[92] In cyberspace, the principle is also

[87] Schmitt (n 27) 55 (Rule 9).
[88] ibid 2–3.
[89] *S.S. Lotus (France v Turkey)* (n 80) 23 ('in a place assimilated to Turkish territory in which the application of Turkish criminal law cannot be challenged, even in regard to offences committed there by foreigners'); Samantha Besson, 'Sovereignty' (2011) *MPEPIL* para 70.
[90] Budapest Convention on Cybercrime (n 49), arts 18(1), 19(1), 19(2), 22(3); Arab Convention on Combating Information Technology Offences (n 70) arts 25, 30(2); GGE Report 2013 (n 69) para 20; CoE PA, 'Mass Surveillance', Doc 13734, 18 March 2015, para 11.
[91] UNGA, Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism (23 September 2014), UN Doc A/69/397, para 41.
[92] *S.S. Lotus (France v Turkey)* (n 80) 23.

recognised as a basis for jurisdiction by conventions governing cybercrimes.[93] While online activities might cross over the jurisdiction of many states, it might be difficult to establish where a cyber activity started and ended. Therefore, the current tendency of state practice is to interpret territorial jurisdiction broadly, where any substantial connection between the cyber activity and state territory might serve as a sufficient basis for jurisdiction.[94]

Related to an area outside the state's effective control, this type of jurisdiction might lead to various scenarios. Under 'objective jurisdiction', the cyber activity originates abroad, but is completed in the area concerned[95] and the territorial state would be entitled, for instance, to exercise its criminal jurisdiction over the perpetrators of the cybercrime by way of mutual legal assistance. Under 'subjective territorial jurisdiction', the state can exercise jurisdiction over any cyber activity originating from the area outside its effective control, such as online recruitment of terrorist fighters or hate speech diffused from the area concerned. Such cyber activities might result in the violation of human rights of victims in the same area, in the government-controlled area, or even in another state.[96]

The third jurisdictional basis proposed by the Tallinn Manual relies on the 'effects doctrine', a jurisdictional link accepted to reflect customary international law:[97] where an activity does not emanate from or end in the state's territory but has effects therein, the state has jurisdiction. While certain domestic courts have applied the effects doctrine to cyberspace,[98] some scholars contest its applicability as it may lead to assertions of jurisdiction in virtually every state by virtue of the accessibility of websites in all countries.[99] The majority doctrine and the International Group of Experts accept its applicability to cyberspace if states use it reasonably, setting a higher threshold of a genuine link between the state and the cyber activity than is applied in the offline world.[100] Accordingly, the territorial state will have jurisdiction over cyber activities that have a substantial effect on the given area, such as the diffusion of online propaganda addressed to the population of the area in their language from abroad.

In other words, the territorial state has jurisdiction under general international law over cyber activities that constitute human rights violations that originate, occur or have an effect in the part

---

[93] Budapest Convention on Cybercrime (n 49) art 22(1)(a); Arab Convention on Combating Information Technology Offences (n 70) art 30(1)(a).

[94] Schmitt (n 27) 57; Inter-American Commission on Human Rights (IACHR), Report of the Special Rapporteur for Freedom of Expression 2013 (31 December 2013), OEA/Ser.L/V/II.149, Doc 50, 496–97, para 66.

[95] Schmitt (n 27) 56 para 5.

[96] Inter-American Judicial Committee (n 64) 164.

[97] Schmitt (n 27) 58.

[98] *LICRA and UEJF v Yahoo! Inc and Yahoo France*, Tribunal de grande instance de Paris, 22 May 2000 and 22 November 2000, No RG:00/0538 (France); High Court of Australia, *Dow Jones and Company Inc v Gutnick* [2002] HCA 56, paras 44, 184, 198–99; *People v World Interactive Gaming Corp*, 22 July 1999, 714 NYS 2d 844, 860, paras 9–10. See other cases cited by Robert Uerpmann-Wittzack, 'Principles of International Internet Law' (2010) 11 *German Law Journal* 1245, 1254–56.

[99] Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 *European Journal of International Law* 799, 811–16; Michael A Geist, 'Is There a There There – Toward Greater Certainty for Internet Jurisdiction' (2001) 16 *Berkeley Technology Law Journal* 1345, 1349.

[100] Joanna Kulesza, *International Internet Law* (Routledge 2012) 14–16; Tsagourias (n 24) 20; Uerpmann-Wittzack (n 98) 1254–56; Schmitt (n 27) 58 para 13. The offline world is understood as activities not connected with cyberspace.

of its territory outside its effective control. The next section examines how the state exercises its jurisdiction in cyberspace under IHRL, where the term 'jurisdiction' has an autonomous meaning.

4. THE STATE'S JURISDICTION UNDER IHRL

As cyberspace is subject to the sovereignty of the state under the jurisdiction rules of general international law referred to above, it is logical to argue that the state is bound by IHRL in cyberspace as it is bound in the offline context. Indeed, states[101] and international organisations[102] have recognised that the rights that people have offline must also be protected online, thus accepting that IHRL applies equally to conduct in cyberspace.[103] While the state has obligations to respect and protect human rights in the cyberspace, it is not clear to what extent it has the same obligations in an area outside its effective control. The two spaces, the online and the physical space, are not completely unrelated, as is shown by the bases of territorial jurisdiction referred to above. In other words, in order to examine how far a state has obligations under IHRL in cyberspace in an area outside its effective control (discussed in Section 5), the preliminary question of how far IHRL applies – through the notion of 'jurisdiction' – to the physical offline space in that area must be clarified.

'Jurisdiction' in IHRL has an entirely different meaning from that of general international law: it is the main criterion for the applicability of international human rights treaties, the nexus between the state and the individual's human rights – that is, the factual control, power or authority that the state exercises over a given individual, territory or situation.[104] Unlike jurisdiction in general international law – defined above as the competence of states to regulate in accordance with international law – jurisdiction in IHRL can be based on a factual situation. This means that in exceptional circumstances jurisdiction can be extraterritorial, covering acts

[101] Budapest Convention on Cybercrime (n 49) art 15(1); 'G8 Declaration Renewed Commitment for Freedom and Democracy', G8 Summit of Deauville, 26–27 May 2011, para II/10, https://www.nato.int/nato_static/assets/pdf/pdf_2011_05/20110926_110526-G8-Summit-Deauville.pdf; NETmundial, 'Multistakeholder Statement', Global Multi-stakeholder Meeting on the Future of Internet Governance, São Paulo, 24 April 2014, Part 1 – Internet Governance Principles: Human Rights and Shared Values, http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf; The White House, 'International Strategy for Cyberspace, Prosperity, Security, and Openness in a Networked World', May 2011, 5, https://info.publicintelligence.net/WH-InternationalCyberspace.pdf.

[102] UNGA Res 68/167 (21 January 2014), UN Doc A/RES/68/167, para 3; UNGA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet (18 July 2016), UN Doc A/HRC/RES/32/13, para 1; UNGA, Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet (14 July 2014), UN Doc A/HRC/RES/26/13, para 1; GGE Report 2013 (n 69) para 21; GGE Report 2015 (n 69) para 26; CoE Committee of Ministers, Recommendation CM/Rec(2016)5[1] to Member States on Internet Freedom, 13 April 2016, para 1.

[103] UN World Summit on the Information Society (n 49) para 1; UN World Summit on the Information Society, Tunis Commitment (18 November 2005), Doc WSIS-05/TUNIS/DOC/7–E, para 2; CoE Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users, 16 April 2014, para 5.1.

[104] De Schutter and others (n 79) 1102 para 3; Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (Oxford University Press 2011) 39.

and omissions of the state authorities performed or which produce effects outside their own territory,[105] even without a lawful basis.[106] However, as a principal rule, international human rights conventions enshrine a primarily territorial notion of jurisdiction, which they apply within the state party's national territory.[107]

The two types of jurisdiction in IHRL, extraterritorial and territorial, leads to the obligations of two states in the cyber context: first, one that effectively controls the territory (Section 4.1), and second, the territorial state (Section 4.2).

4.1. The Jurisdiction of the Outside State

Extraterritorial jurisdiction under IHRL may have two alternative preconditions, based on effectiveness over persons (the personal model):[108] whether cyber activities by a state could give rise to the personal model and, if they could, what is the required level of effectiveness over the person abroad?[109] For present purposes it suffices to note that physical control over foreign territory entails the extraterritorial jurisdiction of the state. It is widely recognised by the International Court of Justice (ICJ)[110] as well as universal[111] and regional[112] human rights treaty monitoring

[105] *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion [2004] ICJ Rep 179 [109]; ECtHR, *Banković and Others v Belgium*, App no 52207/99, Admissibility, 19 December 2001, paras 67–73; Inter-Am Ct HR, *Case of Franklin Guillermo Aisalla Molina (Ecuador) v Colombia (Admissibility)* (2010) Report no 112/10, Inter-state Petition IP-02 of 21 October 2010, (Ser.L) para 98; UN Human Rights Committee, General Comment No 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant [ICCPR] (26 May 2004), UN Doc CCPR/C/21/Rev.1/Add.13, para 10.

[106] eg *Franklin Guillermo Aisalla Molina (Ecuador)*, ibid paras 78–103; ECtHR, *Mansur Pad and Others v Turkey*, App no 60167/00, Admissibility, 28 June 2007, paras 52–55.

[107] *Wall* (n 105) 179 [109]; *Banković* (n 105) para 59; ECtHR, *Al-Skeini and Others v United Kingdom*, App no 55721/07, 7 July 2011, para 131; African Commission on Human and Peoples' Rights (ACommHPR), *Mohamed Abdullah Saleh Al-Asad v Republic of Djibouti*, Case No 383/10, 12 May 2014, para 134; *Franklin Guillermo Aisalla Molina (Ecuador)* (n 105) paras 89–90.

[108] Human Rights Committee, *Sergio Euben Lopez Burgos v Uruguay*, Communication No R.12/52, views of 29 July 1981, UN Doc A/36/40, 182–83 paras 12.1–12.3; Human Rights Committee, General Comment No 31 (n 105) para 10; Inter-American Commission on Human Rights, *Victor Saldaño v Argentina (Admissibility)*, IACHR Report no 38/99, 11 March 1999, OEA/Ser.L/V/II.102 Doc 6 rev, para 21; ECtHR, *Öcalan v Turkey* [GC], App no 46221/99, 12 May 2005, para 91; *Al-Skeini*, ibid paras 134–37.

[109] The International Group of Experts was divided on the question whether only physical power over the person would lead to the personal model that cyber activities are unlikely to reach: Schmitt (n 27) 185 paras 8–9. Some experts claim that even cyber activities below this threshold lead to the imposition of negative obligations to respect: ibid 185–186 para 10; Marko Milanovic, 'Foreign Surveillance and Human Rights, Part 4: Do Human Rights Treaties Apply to Extraterritorial Interferences with Privacy?', *EJIL Talk!*, 28 November 2013, https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-4-do-human-rights-treaties-apply-to-extraterritorial- interferences-with-privacy.

[110] *Wall* (n 105) 179–81 [109]–[113]; *DRC v Uganda* (n 81) 231 [178].

[111] Human Rights Committee, General Comment No 31 (n 105) para 10; UN Committee on the Elimination of Discrimination against Women (CEDAW), General Recommendation No 30 on Women in Conflict Prevention, Conflict and Post-Conflict Situations (1 November 2013), UN Doc CEDAW/C/GC/30, paras 9–10; Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), General Comment No 2: Implementation of Article 2 by States Parties (24 January 2008), UN Doc CAT/C/GC/2, para 16.

[112] ECtHR, *Loizidou v Turkey*, App no 15318/09, Merits, 18 December 1996, para 52; *Cyprus v Turkey*, App no 25781/94, 10 May 2001, paras 77–78; *Al-Skeini* (n 107) paras 138–40; *Franklin Guillermo Aisalla Molina*

bodies that the state is required to fully respect and protect its human rights obligations outside its territory in an area over which it exercises 'effective control' – this is the case of an occupied[113] or leased[114] territory. 'Effective control' is considered to be synonymous with that of 'actual authority',[115] the main requirement of belligerent occupation within the meaning of the 1907 Hague Regulations.[116] Once the state's extraterritorial jurisdiction is established under the spatial model, the state's customary and treaty obligations under IHRL apply also to the cyber context, as monitoring bodies have confirmed.[117] One can add that the area might be effectively controlled not only by a state, but by de facto authorities without the control of an outside state – that is, without their conduct being attributed to a state. As far as they are bound by IHRL,[118] they are obliged to respect human rights in the cyberspace.[119]

4.2. THE JURISDICTION OF THE TERRITORIAL STATE

Beyond an external state having extraterritorial jurisdiction in the area under IHRL, human rights treaty bodies have clarified that the territorial state also continues to have jurisdiction in the part of its territory where it has lost effective control. While extraterritorial jurisdiction is based on effectiveness over territory or over persons, the territorial state's jurisdiction in the absence of its territorial control is based on sovereignty. This can be explained by the general international law presumption of the application of any treaty to the entire territory of the state

(Ecuador) (n 105) paras 101–02; *Mohamed Abdullah Saleh Al-Asad* (n 107) para 134; ACommHPR, *Democratic Republic of Congo/Burundi, Rwanda, Uganda*, Case No 227/99, 29 May 2003, paras 64–65, 76–77.

[113] *Cyprus v Turkey*, ibid para 77; *Al-Skeini* (n 107) para 138; Human Rights Committee, Concluding Observations: Israel (18 August 1998), UN Doc CCPR/C/79/Add.93, para 10; CERD, Concluding Observations: Israel (30 March 1998), UN Doc CERD/C/304/Add.45, para 4; CEDAW, General Recommendation No 28 on the Core Obligations of States Parties under Article 2 CEDAW (16 December 2010), UN Doc CEDAW/C/GC/28, para 39; CEDAW, General Recommendation No 30 (n 111) para 12(c).

[114] Under a territorial lease agreement, the beneficiary state (the lessee) has the right to use and exercise control over the leased territory: Ronen (n 3) para 1.

[115] ECtHR, *Chiragov and Others v Armenia*, App no 13216/05, Merits, 16 June 2015, para 96; Human Rights Council, 'Situation of Human Rights in the Temporarily Occupied Autonomous Republic of Crimea and the City of Sevastopol (Ukraine)' (25 September 2017), UN Doc A/HRC/36/CRP.3, para 38, note 30; Yoram Dinstein, *The International Law of Belligerent Occupation* (Cambridge University Press 2009) 40, 42; Milanovic (n 104) 142.

[116] Hague Convention (IV) Respecting the Laws and Customs of War and its Annex: Regulations Concerning the Laws and Customs of War on Land, *Martens Nouveau Recueil* (ser 3) 461 (entered into force 26 January 1910), art 42.

[117] Human Rights Committee, Concluding Observations: Russian Federation (n 10) para. 23(b); Human Rights Council, Ukraine 2017 (n 7) para 184(b); Human Rights Council (n 115) paras 157, 226(n).

[118] Murray (n 5) 120–71 (Ch 5–6); Fortin (n 16) 240–84 (Ch 9) and 323–56 (Ch 11).

[119] UN monitoring bodies have recommended that de facto authorities respect and protect freedom of expression, including the work of journalists and bloggers: Human Rights Council, Ukraine 2017 (n 7) para 183(h); UN OHCHR, Report on the Human Rights Situation in Ukraine 16 February to 15 May 2015, 38 para (t), https://www.ohchr.org/Documents/Countries/UA/10thOHCHRreportUkraine.pdf; UN OHCHR, Report on the Human Rights Situation in Ukraine 16 May to 15 August 2016, para 210(b), https://www.ohchr.org/Documents/Countries/UA/Ukraine15thReport.pdf; UN OHCHR, Report on the Human Rights Situation in Ukraine, 16 November 2016 to 15 February 2017, para 168(l), https://www.ohchr.org/Documents/Countries/UA/UAReport17th_EN.pdf; Human Rights Council, Mission to Israel (n 7) para 118.

party.[120] In the *Assanidze* case – concerning the difficulty of the Georgian central authorities in enforcing a decision of acquittal by a regional administration – the ECtHR established the 'presumption of competence' or, in other words, the presumption of the state's jurisdiction in respect of its entire territory.[121] While it did not specify whether it is a rebuttable presumption, it referred to objective circumstances that exclude the state's effective control over part of its territory, such as the separatist aspirations of a region or the exercise of effective overall control by another state there.[122] The Court further elaborated on the presumption of jurisdiction in the *Ilasçu* judgment.[123] The case concerned the question of Moldova's jurisdiction for alleged human rights violations committed by the unrecognised de facto authorities of Transnistria, an area within the territory of the Republic of Moldova. The Court held that the presumption of the territorial state's jurisdiction may be limited in exceptional circumstances 'where a State is prevented from exercising its authority in part of its territory' as a result of military occupation by another state, 'acts of war or rebellion, or the acts of a foreign State supporting the installation of a separatist State within the territory of the State concerned'.[124] The same circumstances prevent the territorial state from exercising its authority in the cyberspace as far as it loses control over the physical layers.

The ECtHR did not recognise that the presumption of jurisdiction could be rebutted, but held that it might be 'limited' in such an exceptional situation:[125]

> Those [positive] obligations [undertaken by the states parties under Article 1 of the Convention] remain even where the exercise of the State's authority is limited in part of its territory, so that it has a duty to take all the appropriate measures which it is still within its power to take.

And:[126]

> The Court considers that where a Contracting State is prevented from exercising its authority over the whole of its territory by a constraining *de facto* situation, such as obtains when a separatist regime is set up, whether or not this is accompanied by military occupation by another State, it does not thereby cease to have jurisdiction within the meaning of Article 1 of the Convention over that part of its territory temporarily subject to a local authority sustained by rebel forces or by another State.

In other words, the presumption is irrebuttable, as the territorial state continues to have residual jurisdiction under IHRL. Therefore, the ECtHR held that unilateral declarations made by territorial states by which they intend to exclude the application of the European Convention on Human

---

[120] Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331, art 29. Commentators note that it is a minimum rule of customary character: see Michal Gondek, 'Extraterritorial Application of the European Convention on Human Rights: Territorial Focus in the Age of Globalization?' (2005) 52 *Netherlands International Law Review* 349, 350.
[121] *Assanidze* (n 2) para 139.
[122] ibid para 140.
[123] ECtHR, *Ilaşcu and Others v Moldova and Russia*, App no 48787/99, 8 July 2004.
[124] ibid para 312.
[125] ibid para 313.
[126] ibid para 333.

Rights (ECHR) in its entirety to the area outside their effective control cannot have the effect of restricting the territorial application of the Convention.[127] Certain territorial states made similar declarations while signing the Budapest Convention on Cybercrime – a multilateral treaty binding more than 60 states parties:[128] Azerbaijan, the Republic of Moldova and Ukraine declared their inability to apply the Convention in areas outside their effective control.[129] Unlike the ECHR, which applies to the entire metropolitan territory and allows the extension of its applicability only to dependent territories,[130] Article 38 of the Budapest Convention allows states parties to specify the territory or territories to which the Convention applies and thus exclude certain areas from its territorial scope. However, the Budapest Convention is complementary to and does not affect states parties' applicable multilateral or bilateral treaties,[131] including human rights treaties.[132] Therefore, the non-application of the Budapest Convention to areas outside the state's effective control does not affect the human rights obligations of the territorial state or the scope of its jurisdiction under IHRL.

Beyond confirming the territorial state's jurisdiction, the ECtHR also clarified the kind of positive obligations the territorial state has with regard to individuals in the area outside its effective control. It held that the territorial state is required to take 'appropriate and sufficient' measures in order to guarantee the rights of individuals under the ECHR in an area outside its effective control.[133] The Court stated:[134]

> [S]uch a factual situation reduces the scope of that jurisdiction in that the undertaking given by the state under Article 1 must be considered by the Court only in the light of the Contracting State's positive obligations towards persons within its territory. The state in question must endeavour, with all the legal and diplomatic means available to it vis-à-vis foreign states and international organisations, to continue to guarantee the enjoyment of the rights and freedoms defined in the Convention.

In the case of human rights violations committed by de facto authorities in the area, the ECtHR will verify whether the territorial state has complied with a minimum threshold in the particular circumstances – 'to what extent a minimum effort was nevertheless possible and whether it should have been made'.[135] The territorial state's positive obligations relate both to the measures needed to re-establish its control over its territory 'as an expression of its jurisdiction, and to

[127] ibid paras 20–21; *Assanidze* (n 2) para 140; ECtHR, *Sargsyan v Azerbaijan*, App no 40167/06, Admissibility, 14 December 2011, paras 64–65.
[128] Budapest Convention on Cybercrime (n 49).
[129] Reservations and Declarations for Treaty (n 50).
[130] ECHR (n 29) art 56.
[131] Budapest Convention on Cybercrime (n 49) art 39.
[132] ibid art 15(1).
[133] *Ilaşcu* (n 123) para 334.
[134] ibid para 333.
[135] Ibid para 334.

measures to ensure respect for the applicants' rights'.[136] The obligation to re-establish control over the territory requires the territorial state, 'first, to refrain from supporting the separatist regime and, secondly, to act by taking all the political, judicial and other measures at its disposal for re-establishing control over that territory'.[137]

The second aspect of the territorial state's positive obligation to ensure respect for individuals' rights includes 'the diplomatic, economic, judicial or other measures that it is in its power to take and are in accordance with international law to secure to the applicants the rights guaranteed by the Convention'.[138] The availability of those measures is context-dependent and monitoring bodies will examine their use on a case-by-case basis.

In the *Ilasçu* judgment of the ECtHR six dissenting judges opposed the jurisdiction of Moldova, holding that there was no evidence of the state's direct or indirect authority over, or acquiescence in the commission of the human rights violations in Transnistria.[139] Similarly, some commentators consider the judgment to be too strict with regard to Moldova.[140] However, subsequent case law shows unanimity or an overwhelming majority in the judgments regarding Moldova's responsibility.[141]

It seems that the ECtHR did not set the threshold too high, considering that the judgment cited several concrete examples where the measures taken by the Moldovan government produced real effects on the lives of individuals in Transnistria in general, or the applicants in particular.[142] The measures taken by the territorial state that the Court accepted as complying with its positive obligations consisted, for instance, of diplomatic acts such as protests or negotiation,[143] non-recognition of the illegal situation,[144] investigative or judicial measures operated in the government-controlled area,[145] provision of certain socio-economic benefits for individuals in

[136] ibid para 339; ECtHR. *Catan v Moldova and Russia*, App no 43370/04, 8252/05 and 18454/06, 19 October 2012, para 145; ECtHR, *Mozer v Republic of Moldova and Russia* [GC], App no 11138/10, 23 February 2016, para 151.
[137] *Catan*, ibid para 145; *Mozer*, ibid para 151; *Ilaşcu* (n 123) para 340.
[138] *Ilaşcu* (n 123) para 331.
[139] *Ilaşcu* (n 123) partly dissenting opinion of Judge Sir Nicolas Bratza joined by Judge Rozakis, Judge Hedigan, Judge Thomassen and Judge Panţîru, paras 8–9, 26; partly dissenting opinion of Judge Loucaides.
[140] Thomas D Grant, 'Ukraine v. Russian Federation in Light of Ilaşcu: Two Short Points', *EJIL: Talk!*, 22 May 2014, https://www.ejiltalk.org/ukraine-v-russian-federation-in-light-of-ilascu-two-short-points.
[141] eg *Catan* (n 136) dispositive part, para 3 (unanimous decision); *Mozer* (n 136) dispositive part, paras 6, 8, 11, 13; ECtHR, *Braga v Republic of Moldova and Russia*, App no 76957/01, 17 October 2017, dispositive part, paras 4, 6, 8 (unanimous decisions).
[142] *Ilaşcu* (n 123) paras 345 (improvement of the everyday lives of the people of Transnistria by measures of cooperation), 347 (sending doctors and financial support to the applicants' families, long negotiations with the authorities of the 'MRT' on the liberation of Mr Ilaşcu – see also para 274 and Annex, Mr Sturza, paras 310–12).
[143] ECtHR, *Ivanţoc and Others v Moldova and Russia*, App no 23687/05, 15 November 2011, para 109; *Mozer* (n 136) para 153; ECtHR, *Eriomenco v Republic of Moldova and Russia*, App no 42224/11, 11 December 2017, para 60.
[144] *Ivanţoc*, ibid para 19.
[145] *Catan* (n 136) paras 153, 214–16; ECtHR, *Turturica and Casian v Republic of Moldova and Russia*, App nos 28648/06 and 18832/07, 30 August 2016, para 53; ECtHR, *Paduret v Republic of Moldova and Russia*, App no 26626/11, 9 May 2017, para 33.

the area,[146] and cooperation with other states or international organisations in addressing the wrongful act.[147]

The territorial state's positive obligations arise from the sovereign state's so-called due diligence standard.[148] Under due diligence, 'no state has the right to use or permit the use of its territory in such a manner as to cause injury by fumes in or to the territory of another or the properties or persons therein'.[149] Consequently, the state 'on whose territory or in whose waters an act contrary to international law has occurred, may be called upon to give an explanation' and where the state knew, or ought to have known, of any unlawful act perpetrated in its territory that caused damage to another state, then the first state is obliged to take measures to prevent it or, in the case of a continuing or a terminated violation, to respond to it.[150] Considered also as a customary norm[151] or general principle of law,[152] due diligence has been extended in IHRL as an obligation to protect not only other states, but also individuals against violations by third parties (private parties or other states).[153]

In other words, due diligence is a general international law standard that leads to concrete positive obligations in IHRL to prevent and respond to human rights violations in the territory of the state. Therefore, the relation between the due diligence standard and positive obligations in IHRL is that of the general and the special. The standard is especially applicable to a state having lost its territorial control, as it guarantees flexibility in assessing its particular situation. The state incurs responsibility for failing to comply with due diligence only under two cumulative conditions: (i) it had the means to prevent or to repress the human rights violation; and (ii) it knew or should have known about the risk of the violation.[154] The first condition – known also as the 'capacity to influence' effectively the actions of private actors[155] – assesses the actual means in the state's power to take legal, administrative, diplomatic and other measures to protect human rights. This means that the jurisdiction of the territorial state, while based mainly on sovereignty, still depends on effectiveness as far as the latter determines the scope of the state's obligations. Accordingly, the state is required to take all those steps it reasonably could within its effective power in the particular situation. According to the second condition, the state is responsible only if the human rights violation actually occurred and if the state was aware of, or should

[146] *Catan* (n 136) para 147; ECtHR *Vardanean v Republic of Moldova and Russia*, App no 22200/10, 30 May 2017, para 42.
[147] *Ivanţoc* (n 143) para 109; *Vardanean*, ibid para 42.
[148] *Island of Palmas Case* (n 80) 839.
[149] *Trail Smelter Case (US, Canada)* (1938, 1941) III UNRIAA 1965; in the same sense *Corfu Channel Case (UK v Albania)* (Merits) [1949] ICJ Rep 4, 22.
[150] *Corfu Channel case*, ibid 18.
[151] *Pulp Mills on the River Uruguay (Argentina v Uruguay)* (Merits) [2010] ICJ Rep 14, 55–56 [101].
[152] *Corfu Channel Case* (n 149) 22; Timo Koivurova, 'Due Diligence', (2010) *MPEPIL*, para 2.
[153] *Case of Velásquez Rodríguez v Honduras* (Merits) (1988) Inter-Am CtHR, Judgment of 29 July 1988, (Ser C) No 4, [172].
[154] *Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)* (Merits) [2007] ICJ Rep 43, [430]–[431].
[155] ibid [430].

normally have learned of the risk of the violation.[156] In respect of areas outside the effective control of the state, actual knowledge and available means is to be assessed to establish whether the territorial state complied with its due diligence – as is the practice of the ECtHR in its case law.

It could be argued that the threshold set by the ECtHR in separatist areas is too demanding, binding only on states parties to the ECHR, a regional treaty enshrining one of the highest standards. However, UN Charter-based human rights bodies[157] and universal treaty monitoring bodies[158] have reiterated the same standard and addressed various positive obligations with regard to individuals in areas outside government control in their concluding observations on territorial states.[159] While the ECtHR has based this case law on the necessity to cover the European 'legal space' by the effective application of the ECHR[160] and to eliminate 'vacuums' at the regional level,[161] UN treaty monitoring bodies seek to ensure the universality of human rights with the same practice. The irrebuttable presumption of the territorial state's jurisdiction in IHRL is in conformity not only with the object and the purpose of human rights treaties (the 'legal space' and elimination of the vacuums at the regional level, universality at the universal level), but also with the concept of the 'responsibility to protect' of the territorial state.[162] It is perhaps too early to speak of an established customary norm,[163] but at least international human rights treaties are interpreted in accordance with the above mentioned practice.[164]

The obligation not to allow the state's territory to be used for acts contrary to the rights of other states or individuals binds the state in every activity performed in its territory, including

[156] ibid [431]; *Corfu Channel Case* (n 149) 22 ('the laying of the minefield which caused the explosions on October 22nd, 1946, could not have been accomplished without the knowledge of the Albanian Government').
[157] Human Rights Council (n 115) para 41; Special Rapporteur on Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, 'Mission to the Republic of Moldova' (12 February 2009), UN Doc A/HRC/10/44/Add.3, para 6.
[158] The Human Rights Committee has recently elaborated a general comment, providing that 'a State party has an obligation to respect and to ensure the rights under article 6 of all persons who are within its territory and all persons subject to its jurisdiction'. This wording seems to accept the state's continued jurisdiction in its entire territory despite its lack of effective control over some areas: Human Rights Committee, General Comment No 36 on Article 6 of the International Covenant on Civil and Political Rights, on the Right to Life (30 October 2018), UN Doc CCPR/C/GC/36, para 63. See the wording '[persons] within their territory or effective control': CEDAW, General Recommendation No 28 (n 113) para 12; CEDAW, General Recommendation No 30 (n 111) para 5.
[159] Human Rights Committee, Concluding Observations: Republic of Moldova (4 November 2009), UN Doc CCPR/C/MDA/CO/2, para 5; CAT, Concluding Observations: Republic of Moldova (29 March 2010), UN Doc CAT/C/MDA/CO/2, para 4; UN Committee on the Rights of the Child (CRC), Concluding Observations: Iraq (3 March 2015), UN Doc CRC/C/IRQ/CO/2-4, paras 45, 53(a); CRC, Concluding Observations: Iraq (5 March 2015), UN Doc CRC/C/OPSC/IRQ/CO/1, paras 17(b), 19; CAT, Concluding Observations: Ukraine (12 December 2014), UN Doc CAT/C/UKR/CO/6, para 11(a); Committee on Economic, Social and Cultural Rights, Concluding Observations: Iraq (27 October 2015), UN Doc E/C.12/IRQ/CO/4, para 5.
[160] *Sargsyan* (n 127) paras 147–48 and concurring opinion of Judge Yudkivska; CoE PA (n 8) paras 11, 14.
[161] *Cyprus v Turkey* (n 112) paras 78, 91; *Mozer* (n 136) para 136; ECtHR, *Demopoulos and Others v Turkey*, App nos 46113/99, 3843/02, 13751/02, 13466/03, 10200/04, 14163/04, 19993/04, 21819/04, 2010, para 96.
[162] See nn 61–62.
[163] *a contrario*, in this sense: CRC, Written Replies by the Government of Georgia to the List of Issues (20 May 2008), UN Doc CRC/C/GEO/Q/3/Add.1, para 41.
[164] See nn 158–159.

cyber activities.[165] While the Tallinn Manual discusses extraterritorial jurisdiction in IHRL,[166] it fails to set out the presumption of the state's jurisdiction over its entire national territory. It equally fails to integrate the due diligence standard in IHRL – this would conceptualise the obligation to protect[167] and establish systemic integration between the general and the special regimes of international law applicable to cyber operations. The reason for these omissions is the focus of the Manual on customary rather than conventional IHRL.[168] However, given the almost universal ratification of the various UN human rights treaties and the wide ratification of regional human rights treaties, their convergent treaty practice should be taken into account. As explained in the next section, due diligence and the specific positive obligations it leads to in IHRL – namely, within the territorial state's jurisdiction over human rights violations committed in the area outside its effective control – apply equally in cyberspace.

5. THE APPLICATION OF IHRL BY THE TERRITORIAL STATE IN CYBERSPACE

Certain states have declared their readiness to apply to cyberspace the existing norms of international law, without the need to reinvent a new special branch of international law.[169] This suggests that IHRL is adaptable to new phenomena like cyberspace with its existing normative framework.[170] Because of the horizontal protection they impose against violations by third parties, the due diligence standard and the corresponding positive obligations of the territorial state in IHRL are likely to be adaptable to the online context. Human rights monitoring bodies have recognised that where a state exercises its jurisdiction in the sense of general international law (Section 3) – that is, its regulatory authority over the telecommunications or internet service providers in its territory – the same state is bound by its international human rights obligations.[171] However, they did not specify what the applicable norms are when the state has no effective control over part of its territory.

If the case law of IHRL on the jurisdiction of the territorial state is applied to the cyberspace, it appears that the presumption of its jurisdiction and its positive obligations apply fully in the online context, even in the absence of effective control over the physical infrastructure. As mentioned above, the ECtHR applies a two-step approach to examine whether the territorial state has complied with its positive obligations: its positive obligations relate both to the measures needed to re-establish its control over its territory 'as an expression of its jurisdiction' (Section 5.2), 'and

[165] Karine Bannelier and Theodore Christakis, 'Cyber-Attacks – Prevention-Reactions: The Role of States and Private Actors', Social Science Research Network 2017, SSRN Scholarly Paper ID 2941988 18, https://papers.ssrn.com/abstract=2941988; Schmitt (n 27) 30–43.
[166] Schmitt (n 27) 184–87, 198.
[167] ibid 197–201.
[168] ibid 179–80.
[169] The White House (n 101) 9; AALCO (n 68) para 12 (Malaysia).
[170] Kubo Mačák, 'From Cyber Norms to Cyber Rules: Re-Engaging States as Law-Makers' (2017) 30 *Leiden Journal of International Law* 877, 886.
[171] UNGA, Human Rights Council, The Right to Privacy in the Digital Age (30 June 2014), UN Doc A/HRC/27/37, para 34; Human Rights Committee, General Comment No 34: Article19: Freedom of Opinions and Expression (12 September 2011), UN Doc CCPR/C/GC/34, para 39; UNGA, Report of the Special Rapporteur (n 91) para 41.

to measures to ensure respect for the individual applicants' rights'[172] (Section 5.3). Before examining how these positive obligations apply in cyberspace, the article will explain that, despite the focus of the ECtHR on positive duties, the territorial state is bound equally by negative obligations under IHRL in cyberspace (Section 5.1). As this section will clarify, universal human rights monitoring bodies also share the territorial state's negative and positive obligations.

5.1. Negative Obligations

The emphasis of the ECtHR on positive obligations certainly does not disregard the fact that the territorial state continues to be bound by negative duties. Such duties are understood as the state's obligation not to violate human rights in an area outside its territorial control. Negative obligations continue to impose on the territorial state, for example, the duty not to violate the right to life of individuals by cyber attacks, the prohibition of torture and inhuman or degrading treatment through online means,[173] and prohibitions on freedom of expression, including incitement to racial hatred[174] or to terrorism.[175] In this regard, there is no difference between government-controlled areas and those not under government control: negative obligations bind the territorial state in both contexts.

As mentioned above, territorial states have often had recourse to blocking or filtering communications on the internet, invoking protection of their national security.[176] A first possible legal basis for such measures is the derogation allowed by certain human rights treaties in a state of emergency. Under such a derogation, a state may suspend provisionally the application of one or more human rights, to the extent strictly required by the exigencies of the situation at a time of sufficiently grave crisis that threatens the life of the nation, provided that such measures are not inconsistent with its other obligations under international law.[177] While the territorial state may derogate in respect of certain human rights, such as freedom of expression, it cannot limit

[172] *Ilaşcu* (n 123) para 339; *Catan* (n 136) para 145; *Mozer* (n 136) para 151.
[173] Cyber threats might cause mental suffering of such severity that would violate the prohibition of torture, or inhuman or degrading treatment: ECtHR *Gäfgen v Germany*, App no 22978/05, 1 June 2010, para 108; Human Rights Committee, General Comment No 20: Article 7 (27 May 2008), UN Doc HRI/GEN/1/Rev.9 (Vol I), 200–02 para 5.
[174] CERD (n 30) art 4; ICCPR (n 29) art 20; CERD, General Recommendation No 35: Combating Racist Hate Speech (26 September 2013), UN Doc CERD/C/GC/35.
[175] UNSC Res 2253 (17 December 2015), UN Doc S/RES/2253 (2015), para 22; UNGA, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (10 August 2011), UN Doc A/66/290, para 81.
[176] eg, the Ukrainian presidential decree of 16 May 2017 targeted 'legal entities of the Russian Federation, the activity of which threatens information and cyber security of Ukraine': see Human Rights Committee (n 6) para 95, n 103.
[177] ECHR (n 29) art 15(1); ICCPR (n 29) art 4(1); American Convention on Human Rights (entered into force 18 July 1978) 1144 UNTS 143 (ACHR), art 27(1); Arab Charter on Human Rights (entered into force 15 March 2008), (2005) 12 *International Human Rights Reports* 893, art 4(b).

the application of non-derogable rights,[178] nor the totality of human rights affected by the loss of effective control, and it should regularly review the derogation.[179]

Second, even beyond emergency situations, international human rights treaties permit the lawful restriction of freedom of expression, if prescribed by law and to the extent necessary to ensure national security, territorial integrity, the protection of the rights of others or the prevention of disorder or crime.[180] The protection of the existence of the nation, its territorial integrity and political independence against the use of or threat of force might justify the invocation of national security,[181] provided that the conventional limits of restricting freedom of expression are respected. As the Human Rights Committee held:[182]

> Any restrictions on the operation of websites, blogs or any other internet-based, electronic or other such information dissemination system, including systems to support such communication, such as internet service providers or search engines, are only permissible to the extent that they are compatible with paragraph 3 [of Article 19 of the ICCPR on freedom of expression].

Furthermore, '[p]ermissible restrictions generally should be content-specific; generic bans on the operation of certain sites and systems are not compatible with paragraph 3'.[183] Human rights treaty bodies allow national authorities to restrict a given communication only in proportion to the nature and extent of its perceived threat to national security or other protected interests.[184] In other words, states parties have a negative obligation not to interfere with freedom of expression, unless the restriction is prescribed by law, made in the interests of the admitted legitimate purposes, and satisfies the necessity and proportionality test. The same three-part test applies in situations of armed conflict where international humanitarian law applies simultaneously.[185]

---

[178] ECHR (n 29) art 15(2); ICCPR (n 29) art 4(2) and Second Optional Protocol (entered into force 11 July 1991) 999 UNTS 414, art 6; Human Rights Committee, General Comment No 29: States of Emergency (Article 4) (31 August 2001), UN Doc CCPR/C/21/Rev.1/Add.11, paras 8, 13, 15; ACHR, ibid arts 4(c), 27(2).

[179] ECHR (n 29) art 15(3); ECtHR, *Brannigan and McBride v United Kingdom*, App nos 14553/89 and 14554/89, 23 May 1993, para 54; ICCPR (n 29) art 4(3); ACHR (n 177) art 27(3); Human Rights Committee, General Comment No 29, ibid para 4.

[180] ECHR (n 29) art 10(2); ICCPR (n 29) art 19(3)(b); ACHR (n 177) art 13(2)(b); *a contrario*, see, without any express limitation, African Charter on Human and Peoples' Rights, art 9 (for the implied limitations, see below n 184).

[181] 'The Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights Symposium: Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights: Principles' (1985) 7 *Human Rights Quarterly* 3, 6 para 29.

[182] Human Rights Committee, General Comment No 34 (n 171) para 43.

[183] ibid.

[184] Human Rights Committee, *Keun-Tae Kim v Republic of Korea*, Communication No 574/1994, views of 4 January 1999, UN Doc CCPR/C/64/D/574/1994, paras 12.4–12.5; and *Jong-Kyu Sohn v Republic of Korea*, Communication No 518/1992, 3 August 1995, UN Doc CCPR/C/54/D/518/1992, para 10.4; ECtHR, *Jankovskis v Lithuania*, App no 21575/08, 17 January 2017, paras 61–63; ECtHR, *Ahmet Yıldırım v Turkey*, App no 3111/10, 18 December 2012, para 66 and concurring opinion of Judge Pinto de Albuquerque; AfrCtHPR, *Ingabire Victoire Umuhoza v Republic of Rwanda*, App no 003/2014, Judgment of 24 November 2017, [161]–[162].

[185] OSCE, Joint Declaration on Freedom of Expression and Responses to Conflict Situations (4 May 2015), UN/OSCE/OAS/ACHPR, para 2(c), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=15921&LangID=E.

Unqualified and broadly defined monitoring of the content of internet communications, such as nationwide filtering measures, is likely to be considered an unlawful restriction of freedom of expression and the right of access to information.[186] The *a posteriori* (after publication) blocking or filtering of clearly specified unlawful content can be considered lawful, however, to protect the rights and interests of others and of society as a whole if the above-mentioned conditions of permitted restrictions are satisfied, even without notice from the alleged victims or from third parties.[187]

5.2. Measures Intended to Re-establish Control over Territory/Cyberspace

As mentioned above, the territorial state is required to take all political, judicial and other measures at its disposal for re-establishing control over its territory. Such measures serve as mere expression of its jurisdiction over areas not under government control,[188] irrespective of the ineffectiveness of those measures: the ECtHR has also recognised that there might be little that the territorial state could do to re-establish its authority over the area.[189] Such measures could be considered to be 'pure political rhetoric'[190] or the mere expression of the state's desire to re-establish its territorial control, which is incapable of being subjected to judicial review.[191] While it is indeed difficult to derive such an obligation from IHRL which protects individuals rather than state sovereignty, it can be seen as part of the due diligence standard. The latter standard, that of the '*diligens paterfamilias*',[192] would expect any reasonable, civilised government, as a minimum, to refrain from acquiescing in the wrongful acts,[193] and to reassert its responsibility for its national territory and its residents.

The expected measures may consist of asserting sovereignty over the area 'both internally and internationally'; criminal proceedings against certain leaders of the de facto authorities; diplomatic negotiations; or certain forms of cooperation with the de facto authorities with a view to normalising the everyday lives of the people living in the area.[194] The measures to re-establish control over territory apply to the online context as far as control over cyberspace and extending access to the internet ensure a greater likelihood of human rights protection by the territorial

[186] *Ahmet Yıldırım v Turkey* (n 184) paras 66–69; ECtHR, *Szabó and Vissy v Hungary*, App no 37138/14, 12 January 2016, paras 62–89; Case C-70/10 *Scarlet Extended SA v Société belge des auteurs* [2011] ECR I-11959, [47]–[54]; Human Rights Committee, Concluding Observations: Islamic Republic of Iran (29 November 2011), UN Doc CCPR/C/IRN/CO/3, para 27; Human Rights Committee, Concluding Observations: Turkmenistan (19 April 2012), UN Doc CCPR/C/TKM/CO/1, para 18.
[187] ECtHR, *Delfi AS v Estonia* [GC], App no 64569/09, 16 June 2015, paras 153, 159.
[188] *Ilaşcu* (n 123) para 339.
[189] ibid para 341.
[190] Ganna Yudkivska, 'Territorial Jurisdiction and Positive Obligations of an Occupied State: Some Reflections on Evolving Issues under Article 1 of the European Convention' in Van Aaken and Motoc (n 7) 136, 143.
[191] Marko Milanovic and Tatjana Papić, 'The Applicability of the ECHR in Contested Territories' (2018) 67 *International and Comparative Law Quarterly* 779, 796.
[192] *Negrete* case, cited in John Bassett Moore, *A Digest of International Law* (Goverment Printing Office 1906) 962.
[193] *DRC v Uganda* (n 81) [300], and Declaration of Judge Tomka, [2]–[3].
[194] *Ilaşcu* (n 123) paras 341–45.

state.[195] The internet is a channel through which the state can fulfil human rights, such as the right to education, the right to vote and the right to an effective remedy for citizens from the area outside the state's effective control.[196] Therefore, measures that aim to re-establish 'internet sovereignty' are likely to satisfy the requirements of the ECtHR. For instance, diplomatic protests against the ongoing violation of the state's sovereignty over cyberspace in the area,[197] the expression of an intention to re-establish its control in a treaty declaration on the Budapest Convention on Cybercrime,[198] cooperation with the de facto authorities to restore telecommunication links,[199] or the restoration of a transmission tower in the neighbourhood of the area not under government control[200] are likely to constitute measures intended to re-establish control over sovereignty/cyberspace.

As a general rule, the state has a discretion to choose the measures to re-establish control that it deems the most appropriate. However, it is problematic if the state restricts internet/telecommunications for an extended period in order to re-assert control over its territory, while the same measures violate individuals' human rights and thus run against the third type of obligation (below). For instance, in the context of the Iraqi fight against online propaganda and terrorist recruitment by ISIL, the Iraqi government ordered internet service providers to shut down the internet in the five provinces under ISIL control in June 2014.[201] In fact, the measures aimed to re-establish control over territory/cyberspace should be taken within the limits defined by international law[202] in general, and IHRL in particular. The three-part test referred to above determines the lawful restriction of qualified human rights, especially freedom of expression. While blocking websites that are dedicated to inciting racial discrimination and hatred in conformity

[195] UNGA, Report of the Special Rapporteur (n 175) paras 61, 88; Human Rights Council (n 49) paras 2, 3, 5; OSCE (n 185) paras 4, 6(a).

[196] For some good practices of Ukrainian relocated courts see OSCE Special Monitoring Mission to Ukraine, 'Access to Justice and the Conflict in Ukraine', December 2015, 18–19, https://www.osce.org/ukraine-smm/212311.

[197] 'Declaration of the Ministry of Information Policy of Ukraine', in World Summit on Information Society Forum 2018: High-Level Track Outcomes and Executive Brief, 287–90; International Telecommunication Union (ITU) and ACTF, 'Final Acts of the Plenipotentiary Conference (Busan, 2014): Decisions and Resolutions', 2016, Declarations no 2 (Georgia) and 76 (Ukraine).

[198] For the principle under the ECHR: *Ilaşcu* (n 123) para 343. See the similar declaration of Ukraine to the Budapest Convention ('until the complete restoration of the constitutional law and order and effective control by Ukraine'): Reservations and Declarations for Treaty No 185 (n 50).

[199] *Decizia protocolară cu privire la organizarea interacțiunii în domeniul telecomunicațiilor* [Protocol Decision on Measures to Organize Interaction in the Field of Telecommunications], 25 November 2017, https://gov.md/sites/default/files/2017_11_25_protokolnoe_reshenie_o_vzaimodeystvii_v_oblasti_telekommunikaciy_2.pdf [in Russian]; Protocol of the Official Meeting of the Permanent Conference for Political Questions in the Framework of the Negotiating Process on the Transdniestrian Settlement, 29–30 May 2018, para 6, https://www.osce.org/chairmanship/382885?download=true.

[200] UN OHCHR, Ukraine 16 November 2016 to 15 February 2017 (n 119) para 94.

[201] 'Iraq Telecom Ministry Orders ISPs: Kill The Internet in Five Provinces' (n 47).

[202] *Ilaşcu* (n 123) para 331. The ICJ has recognised, interpreting the obligation of due diligence to prevent genocide, that 'it is clear that every State may only act within the limits permitted by international law': *Bosnia and Herzegovina v Serbia and Montenegro* (n 154) 221 [430].

with fair trial guarantees might be proportionate,[203] shutting down the entire internet in an area outside the territorial state's control is likely to constitute a disproportionate restriction.[204]

5.3. Measures Intended to Ensure Respect for Individuals' Rights

While cyberspace is considered largely as embodying freedom of internet communication, the free flow of information and respect for the right to freedom of opinion and expression,[205] entailing mainly negative obligations on the part of the state, does not exclude positive obligations to protect individuals against human rights violations by third parties. In recent years, human rights treaty monitoring bodies have clarified various positive obligations that states have in cyberspace.[206]

As mentioned above, in areas outside the effective control of the state special measures with the aim of protecting the rights of individuals include positive duties 'to take the diplomatic, economic, judicial or other measures that were both in its power to take and in accordance with international law'.[207] As a translation of the due diligence standard, the anticipated measures depend on the context and must be reasonable – commensurate with the territorial state's limited ability to protect human rights in an area outside its effective control.[208] In the face of online human rights violations, the most relevant measures are providing remedies (5.3.1) and preventive measures (5.3.2).

5.3.1. Providing Remedies

As the territorial state does not have physical access to the elements of the breach (the victim, the perpetrator or the ICT infrastructure) situated in the area, its judicial and investigative authorities are limited to the area under the control of the government. Its obligation to provide remedies should consist of enabling the victim to inform the state authorities 'of the details of his situation and to be kept informed of the various legal and diplomatic actions taken'.[209] It may be possible to enable individuals to seek a remedy remotely, such as by allowing files to be sent

[203] CERD, Concluding Observations: Germany (30 June 2015), UN Doc CERD/C/DEU/CO/19–22, para 9(c).
[204] Human Rights Committee, General Comment No 34 (n 171) para 43; Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (30 March 2017), UN Doc A/HRC/35/22, paras 8–16; OSCE, Joint Declaration on Freedom of Expression and the Internet, 1 June 2011, para 6(b), http://www.osce.org/fom/78309.
[205] Iginio Gagliardone and others, *Countering Online Hate Speech* (UNESCO 2015) 5; ECtHR, *KU v Finland*, App no 2872/02, 2 December 2008, para 49 (recognising freedom of expression and confidentiality of communications for users of telecommunications and internet services as 'primary considerations' on the one hand, and the state's positive obligations to reconcile the various human rights which compete for protection in the cyberspace on the other).
[206] eg, ECtHR, *KU v Finland*, ibid paras 46–49; ECtHR, *Féret v Belgium*, App no 15615/07, 16 July 2009, paras 72–73, 78; ECtHR, *Delfi AS v Estonia* [GC], App no 64569/09, 16 June 2015, para 159; Human Rights Committee, General Comment No 34 (n 171) para 15.
[207] *Ilaşcu* (n 123) para 340; *Catan* (n 136) paras 109–110; *Mozer* (n 136) paras 99–100.
[208] *Mozer* (n 136) para 216.
[209] ibid para 214.

electronically, providing information about remedies and communicating via Skype or email with citizens from the area outside its effective control.[210] Similarly, universal treaty bodies have recommended that states guarantee access to toll-free helplines for victims in all regions within their territory.[211] Another way of complying with the obligation to provide a remedy is to create, in the government-controlled territory, 'a set of judicial, investigative and civil service authorities which work in parallel' with those created by the de facto authorities.[212] While the effects of any decisions taken by these authorities can be felt only outside the conflict area, they have the function of enabling cases to be brought in the proper manner before the territorial state's authorities, 'which can then initiate diplomatic and legal steps to attempt to intervene in specific cases'.[213]

The territorial state is required to undertake to investigate cybercrimes committed in the area outside its effective control.[214] Even though denied access to the area, the territorial state should initiate all investigative procedures commensurate with its limited ability,[215] for instance, by keeping thorough documentation on the victims of human rights violations.[216] The absence of territorial control and access to evidence on the spot is in itself a less important obstacle in the case of cyber activities than in the case of offline human rights violations, because the former can be investigated from remote places. As a first channel, the authorities of the territorial state can monitor publicly available (open source) stored computer data.[217] A second method of investigation is through mutual legal assistance requested from a third state where information technology storing relevant data is located.[218] However, states hosting the largest cyber service providers like the United Kingdom or the United States rarely allow the sharing of digital evidence and might impose restrictions on companies sharing content data with foreign

[210] For some good practices of Ukrainian relocated courts see OSCE (n 196); *Mozer* (n 136) para 214.
[211] CRC, Concluding Observations: Georgia (9 March 2017), UN Doc CRC/C/GEO/CO/4, para 24(e); CEDAW, Concluding Observations: Azerbaijan (12 March 2015), UN Doc CEDAW/C/AZE/CO/5, para 23(d).
[212] *Mozer* (n 136) para 215.
[213] ibid.
[214] In the same sense see certain NGOs: Promo-LEX, 'Resolution on Ensuring and Guaranteeing Free and Secure Internet Access to all Citizens of the Republic of Moldova, including the Transnistrian Region', 2016, https://promolex.md/wp-content/uploads/2016/08/Resolution.pdf.
[215] eg, *Mozer* (n 136) paras 215–16; ECtHR, *Draci v Republic of Moldova and Russia*, App no 5349/02, 17 October 2017, para 61; ECtHR, *Stomatii v Republic of Moldova and Russia*, App no 69528/10, 18 September 2018, paras 71–72.
[216] In their non-binding concluding observations, the treaty bodies have interpreted the duty to investigate violations of physical integrity (torture, enforced disappearance) in this sense: eg, CAT, Concluding Observations: Ukraine (n 159) para 11(a); CAT, Concluding Observations: Iraq (7 September 2015), UN Doc CAT/C/IRQ/CO/1, para 12(b) (victims of inhuman treatment); Committee on Enforced Disappearances, Concluding Observations: Iraq (13 October 2015), UN Doc CED/C/IRQ/CO/1, para 23.
[217] Budapest Convention on Cybercrime (n 49) art 32(a); Arab Convention on Combating Information Technology Offences (n 70) art 40(1).
[218] eg, Budapest Convention on Cybercrime (n 49) arts 29(1), 31(1), 33(1); Arab Convention on Combating Information Technology Offences (n 70) arts 37, 39, 41. Statistics on the frequency of mutual assistance to access stored computer data are available from some state parties to the Budapest Convention: see CoE, Cybercrime Convention Committee (T-CY), 'T-CY Assessment Report: The Mutual Legal Assistance Provisions of the Budapest Convention on Cybercrime', T-CY(2013)17 rev, 3 December 2014, 6, https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c.

governments.[219] Universal human rights monitoring bodies, however, require states in general,[220] and the UK[221] and the US[222] in particular, to strengthen international cooperation in combating certain transnational crimes.[223]

A third channel of investigation in the absence of territorial control is the possibility for states to access computer data stored in another state without obtaining authorisation from that state. This is foreseen in certain cybercrime conventions which allow a party to access stored computer data located in the states of another party with 'the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system'.[224] However, this practice is highly contested on account of its restriction of privacy and the sovereignty of the third state,[225] and the said cybercrime conventions have a limited number of ratifications.[226] A fourth possible channel of investigation is to seek the assistance of international organisations,[227] especially those conducting a programme against cybercrimes such as INTERPOL,[228] EUROPOL,[229] the International Telecommunications Union (ITU),[230] and the Virtual Global Taskforce as an international collaboration combating online child sexual abuse.[231] Furthermore, beyond international cooperation, the territorial state is obliged to seek cooperation with the de facto investigative authorities in crimes concerning the physical integrity of persons (the right to life, prohibition of torture and other inhuman or degrading treatment or

[219] David P Fidler, 'Cyberspace, Terrorism and International Law' (2016) 21 *Journal of Conflict and Security Law* 475, 489–90.
[220] Human Rights Council, Resolution 31/7, Rights of the Child: Information and Communications Technologies and Child Sexual Exploitation (20 April 2016), UN Doc A/HRC/RES/31/7, paras 10–11.
[221] CRC, Concluding Observations: United Kingdom of Great Britain and Northern Ireland (8 July 2014), UN Doc CRC/C/OPSC/GBR/CO/1, para 42.
[222] Special Rapporteur on the Sale of Children, Child Prostitution and Child Pornography, 'Mission to the United States of America' (7 February 2011), UN Doc A/HRC/16/57/Add.5, para 115; CRC, Concluding Observations: United States of America (12 July 2017), UN Doc CRC/C/OPSC/USA/CO/3-4, para 42.
[223] In particular, torture, human trafficking, child sexual exploitation online and violations of the right to life.
[224] Budapest Convention on Cybercrime (n 49) art 32(b); Arab Convention on Combating Information Technology Offences (n 70) art 40(2).
[225] CoE, Cybercrime Convention Committee (T-CY), 'T-CY Guidance Note 3: Transborder Access to Data (Article 32)', T-CY (2013)7 E, 3 December 2014, 8, https://rm.coe.int/16802e726a; Ian Brown and Douwe Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' (2014) *European Human Rights Law Review* 243, 249–50.
[226] While the Budapest Convention on Cybercrime (n 49) has 60, the Arab Convention on Combating Information Technology Offences (n 70) has 8 state parties, as at June 2018.
[227] *Vardanean* (n 146) para 42; ECtHR, *Turturica and Casian v Republic of Moldova and Russia*, App no 28648/06 and 18832/07, 30 August 2016, para 53; ECtHR, *Khlebik v Ukraine*, App no 2945/16, para 80 (referring to the International Committee of the Red Cross); CRC, Concluding Observations: Iraq (4 February 2015), UN Doc CRC/C/OPAC/IRQ/CO/1, para 26(c).
[228] INTERPOL, 'Supporting Digital Crime Investigations', March 2017, http://www.interpol.int.
[229] EUROPOL, 'European Cybercrime Centre (EC3)', https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
[230] ITU, 'ITU Global Cybersecurity Agenda', https://www.itu.int/itunews/manager/display.asp?lang=en&year=2008&issue=09&ipage=18&ext=html.
[231] This consists of law enforcement agencies and partners, which include INTERPOL, EUROPOL and a number of private sector partners: Virtual Global Taskforce, https://virtualglobaltaskforce.com/about/what-is-the-vgt.

punishment).[232] Despite strong contestation of this duty,[233] it is the existing threshold, at least in Europe. For less serious online human rights violations, one can argue that the territorial state should consider seeking cooperation with the de facto authorities.[234] The choice of the concrete forms of investigation depends on the context, but the state should use all available lawful means.

Given that these measures originate from the due diligence standard, under this standard the required degree of diligence depends upon the actual control the territorial state has over cyberspace, its available resources, its capacity to influence the perpetrator effectively and the gravity of the harm.[235] In the cyber context, this means that during an ongoing armed conflict with grave human rights violations offline, while a territorial state like Ukraine might not have the capability to investigate an alleged hacking of e-mail in Eastern Ukraine, it should focus on serious and large-scale human rights violations, such as racial hatred, through the internet.[236] Likewise, when the Iraqi authorities have to allocate their limited investigative capacity among various major human rights violations, it is legitimate that they focus on the online sale of girls[237] as that relates to ongoing violations of the victims' physical integrity to the detriment of less serious breaches of media freedom.

5.3.2. PREVENTIVE MEASURES

It has been queried whether states have a customary international law obligation to prevent wrongful acts in the cyber context.[238] The majority of experts are of the view that the due diligence standard does not impose on states a general obligation of prevention before the cyber activity generates serious adverse effects, but expects the state to stop ongoing wrongful acts

[232] ECtHR, *Güzelyurtlu and Others v Cyprus and Turkey* [Chamber], App no 36925/07, 4 April 2017, paras 291, 293–96; ECtHR, *Güzelyurtlu and Others v Cyprus and Turkey* [GC], App no 36925/07, 29 January 2019, paras 237–38, 241–57. The difference between the rulings of the Chamber and the Grand Chamber is the extent to which the state is expected to take reasonable steps to cooperate. Contrary to the Chamber, the Grand Chamber held that supplying the whole investigation file to the de facto authorities would be unreasonable, as it 'would amount in substance to a transfer of the criminal case by Cyprus to the "TRNC" courts, and Cyprus would thereby be waiving its criminal jurisdiction' over the crime: ibid para 253; *a contrario*, considering the majority judgment as the rejection of the territorial state's procedural obligation to cooperate with the TRNC, see the partly dissenting opinion of Judges Karakaş and Pejchal, para 11.

[233] *Güzelyurtlu* [Chamber], ibid para 238 (Republic of Cyprus) and partly dissenting opinion of Judge Serghides, para 47(h), (o); *Güzelyurtlu* [GC], ibid paras 207–08 (Republic of Cyprus).

[234] CEDAW, Concluding Observations: Georgia (24 July 2014), UN Doc CEDAW/C/GEO/CO/4-5, para 13; Olga Demian, 'Strengthening the Respect for Human Rights in the Implementation of the Republic of Moldova's Digital Agenda, Report on Human Rights Protection on the Internet', CoE Consultant, December 2015, para 7.1.12, https://rm.coe.int/1680630e59, 67.

[235] *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v USA)*, Merits, Judgment, [1986] ICJ Rep 14, 85 [157]; *Bosnia and Herzegovina v Serbia and Montenegro* (n 154) 221 [430].

[236] CERD, Concluding Observations: Ukraine (4 October 2016), UN Doc CERD/C/UKR/CO/22-23, para 12.

[237] CRC, Concluding Observations: Iraq (n 159) para 19(b); on online slave auctions by ISIL, see Human Rights Council (n 58) paras 57, 118.

[238] In favour of such an existing customary norm, Sklerov (n 18) 71; in favour of an 'emerging norm', Erik Talbot Jensen, 'Cyber Sovereignty: The Way Ahead' (2015) 50 *Texas International Law Journal* 275, 299; Bannelier-Christakis (n 18) 32–36.

in cyberspace.[239] IHRL, however, enshrines special duties of prevention that are not limited to the duty to react to and repress ongoing human rights violations in cyberspace, but expects effective measures to prevent violations by third parties if there are reasonable grounds to believe that such abuse will occur.[240]

Human rights monitoring bodies have interpreted various treaty provisions as requiring preventive measures to combat online human rights violations in ordinary situations of governmental control over territory. Their recommendations include, for example, that states parties regularly monitor and prevent incidences of (cyber-)bullying;[241] identify internet service providers with a view to preventing the sale of children, child prostitution and child pornography;[242] collaborate with the media and the ICT industry to enforce global standards for child protection;[243] establish 'effective mechanisms for identifying potential future threats of terrorist attacks before they have materialized' through the gathering and analysis of relevant information by intelligence and law enforcement agencies.[244] The general rule is that the territorial state is required to take all measures within its power as far as their effects might affect areas that are not under government control.

Furthermore, online human rights violations should be prevented by regulatory means,[245] for example, by criminal legislation adopted in the government-controlled area that extends its regulatory scope to the entire territory.[246] The rationale is the preventive effect of the law, even if it is enforceable in the government-controlled area only. For example, the customary international law duty on the part of states to prohibit and prosecute the online recruitment of children, at least under 15 years, into armed forces or armed groups applies to the entire territory.[247]

A state can always regulate internet service providers or online media companies based in the government-controlled area. Human rights treaty bodies recommend 'identify[ing] Internet

[239] Schmitt (n 27) 44–45 paras 8–9; Michael N Schmitt, 'In Defense of Due Diligence in Cyberspace' (2015) 125 *Yale Law Journal Forum* 68, 75–76; Eric Talbot Jensen and Sean Watts, 'A Cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer?' (2017) 95 *Texas Law Review* 1555, 1573. However, it is not disputed that once the harmful cyber conduct has materialised, and the state knew or ought to have known that the harmful conduct was emanating from its territory, it has a duty to take all reasonable measures to terminate that conduct and mitigate its harmful effects: see, eg, Buchan (n 18) 431–32.

[240] Schmitt (n 27) 198–99 para 8.

[241] CRC, Concluding Observations: United Kingdom (12 July 2016), UN Doc CRC/C/GBR/CO/5, paras 49(a)–(b); CRC, Concluding Observations: Bulgaria (21 November 2016), UN Doc CRC/C/BGR/CO/3-5, para 28(f).

[242] CRC, Concluding Observations: Belarus (8 April 2011), UN Doc CRC/C/OPSC/BLR/CO/1, para 27; CRC, Concluding Observations: Montenegro (1 November 2010), UN Doc CRC/C/OPSC/MNE/CO/1, paras 26(c), (e); CRC, Concluding Observations: Bosnia and Herzegovina (25 October 2010), UN Doc CRC/C/OPSC/BIH/CO/1, para 45.

[243] CRC, General Comment No 13 (18 April 2011), UN Doc CRC/C/GC/13, para 43(a)(viii).

[244] Human Rights Committee, Framework Principles for Securing the Human Rights of Victims of Terrorism (4 June 2012), UN Doc A/HRC/20/14, para 21; UNGA, Report of the Special Rapporteur (n 91) para 33.

[245] eg, online harassment and psychological violence: CEDAW, Concluding Observations: Iceland (10 March 2016), UN Doc CEDAW/C/ISL/CO/7-8, para 20(d).

[246] CAT, Concluding Observations: Iraq (n 216) para 28.

[247] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, *Vol 1: Rules* (International Committee of the Red Cross and Cambridge University Press 2005, revised 2009) 485–88.

service providers (ISPs) that host or disseminate offending material'[248] with a view to preventing or mitigating human rights violations. This would be effective as far as those companies provide services in the area outside the government's control. For instance, the Iraqi government could regulate the conduct of those ISPs in the ISIL-controlled areas that were based in the government-controlled territory. As Baghdad does not have centralised control over the country's telecommunications infrastructure, such regulatory measures could not prevent terrorist communication using the service of ISPs based in Turkey and Iran.[249] With regard to those private actors, due diligence would expect Iraq to use all available means, such as requesting legal assistance from its neighbours, even if its efforts are unsuccessful.[250] In the case of belligerent occupation, however, where the territorial state no longer has de facto regulatory power over ISPs, preventive measures might be limited to diplomatic protests and the seizure of international human rights control mechanisms.[251]

While preventing certain online human rights violations, the state should ensure a balance between the limitations of the various human rights. In the case of restricting online content to prevent racial hatred, freedom of expression may be restricted only by applying the three-point test. In the example referred to above of shutting down the internet in five Iraqi provinces under ISIL control, a lawful preventive measure could have involved ordering Iraqi internet service providers to disrupt the use of specific websites and social media by those associated with extremist groups for delivering propaganda and recruiting foreign terrorist fighters.[252]

While the above measures are not exhaustive, human rights control bodies will verify whether a minimum effort was taken by the territorial state to protect human rights online.[253] The threshold of the positive obligations described above, in accordance with due diligence, depends on the actual knowledge and the available means of the territorial state to prevent and mitigate the commission of wrongful acts by third parties. If the state is not aware of the online human rights violations committed against a victim in the area outside its control, it cannot be expected to take positive measures to protect the victim.[254]

The greater the capacity that the state has to comply with its due diligence, the higher is the standard of action required in the particular case. None of those factors – the legal, political,

[248] CRC, Concluding Observations: Belarus (n 242) para 27; in the same sense, CRC, Concluding Observations: Montenegro (n 242) para 26(c); CRC, Concluding Observations: Bosnia and Herzegovina (n 242) para 45.
[249] Shane Harris, 'Iraqi Government Takes Its Fight with ISIS Online', *Foreign Policy*, 17 June 2014, https://foreignpolicy.com/2014/06/17/iraqi-government-takes-its-fight-with-isis-online.
[250] ECtHR, *Soyma v Republic of Moldova, Russia and Ukraine*, App no 1203/05, paras 38–39; *Draci* (n 215) para 61.
[251] With regard to online racial discrimination against the Crimean Tatar media, for instance, NGOs recommended that the Ukrainian government seize both the UN CERD and the ICJ: Oleksandr Burmahyn and others, *Hate Speech in the Media Landscape of Crimea: An Information and Analytical Report on the Spread of Hate Speech on the Territory of the Crimean Peninsula (March 2014 – July 2017)* (Crimean Human Rights Group 2018) 37.
[252] Chair of the Security Council Committee pursuant to Resolutions 1267 (1999) and 1989 (2011) (19 May 2015), UN Doc S/2015/358, para 76(g).
[253] *Ilaşcu* (n 123) para 334.
[254] ECtHR, *Apcov v Moldova and Russia*, App no 13463/07, 30 May 2017, para 46; *Soyma* (n 250) paras 38–39.

administrative, technological, military and diplomatic means – depends exclusively on territorial control that the state has lost in the region in question, but the scope of feasible measures is always context dependent. Feasibility depends, among others, 'on the technical wherewithal of the state concerned, the intellectual and financial resources at its disposal, the state's institutional capacity to take measures, and the extent of its control over cyber infrastructure' located in the government-controlled territory.[255]

This capacity is to a large extent technical, often referred to as 'virtual power'[256] or 'virtual control', understood as the 'ability to intercept, store, analyse and use communications'.[257] Since governments might have very different relationships with the internet and telecommunications companies that could facilitate surveillance, their capacity to access directly the undersea cables and other carriers of internet and telephonic communications might be different. However, 'virtual power' or 'virtual control' is not the only factor that determines the capacity of the territorial state to comply with its due diligence. Even if the state is not a developed state with modern technical infrastructure, it might still have legislative or diplomatic means, for example, to exert pressure on the perpetrators to cease the violation or to prosecute them. Many of the above-mentioned preventive, regulatory, investigative and redress measures can be taken in the government-controlled areas and this fact relativises the importance of the lack of territorial control over the area.

6. CONCLUSIONS

The lack of control of the territorial state over the physical space is closely associated with online human rights violations on the one hand, and the state's restricted (but not necessarily non-existent) control over the cyberspace on the other. Notwithstanding the absence of its effective territorial control, the state continues to be entitled to exercise its sovereignty over both the territory and the cyberspace. The consequence of sovereignty in IHRL is the presumed jurisdiction of the territorial state. The irrebuttable presumption of the state's jurisdiction over its entire territory in IHRL is in conformity not only with the object and the purpose of human rights conventions (the 'legal space' and the elimination of vacuums at the regional level, universality at the universal level), but also with the concept of 'responsibility to protect'. In accordance with the latter theory, it is the primary responsibility of the territorial state to guarantee human rights in its territory.

---

[255] Schmitt (n 27) 47 para 16; in general international law, see the same factors reiterated in *Bosnia and Herzegovina v Serbia and Montenegro* (n 154) [430]; *US Diplomatic and Consular Staff in Tehran*, Judgment [1980] ICJ Rep 3, 31–33 [63]–[68]; *DRC v Uganda* (n 81) 268 [301].

[256] Eliza Watt, 'The Role of International Human Rights Law in the Protection of Online Privacy in the Age of Surveillance' in H Rõigas and others (eds), *2017 9th International Conference on Cyber Conflict: Defending the Core* (NATO CCD COE Publication 2017) 102.

[257] ibid 103. The notion was first used by Margulies, who defines it as an attribution test, the provision of 'financial or other assistance to private groups' by a state: Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 *Melbourne Journal of International Law* 496, 514–15.

Treaty monitoring bodies recommend various positive measures that any territorial state should take while seeking to restore its 'internet sovereignty' in the separatist region – measures disposed to re-establish control over the cyberspace. The territorial state is obliged to use its investigative and judicial capabilities, legislate and regulate non-state actors in the entire national territory, and seek international cooperation in reacting to online human rights violations.

As a result of technological progress, the presumption of the territorial state's jurisdiction is *a fortiori* applicable to cyberspace where the state can ensure the re-establishment of its control over human rights violations, even in the absence of territorial control. Given that most territorial states retain some information and telecommunications infrastructures in their government-controlled area, applying the so-called due diligence standard to human rights in cyberspace in areas outside the effective control of the territorial state is feasible. Consequently, national legislation, cyber security strategies, military manuals and doctrinal commentaries like the Tallinn Manual[258] should expressly recognise that the state is presumed to have jurisdiction under IHRL over its entire territory, even in the absence of effective control over it.

A revised Tallinn Manual should integrate the due diligence standard in its chapter on IHRL with a view to conceptualising the obligation to protect[259] and establish systemic integration between the general and the special regimes applicable to cyber operations. More generally, it should further take into account the obligations flowing from international human rights treaties, especially those applied universally.

[258] Schmitt (n 27) 182–84 (rule 34 – Applicability).
[259] ibid 197–201.