UNIVERSITY OF ESSEX **DISSERTATION**

SCHOOL OF LAW

LLM/MA IN: LLM International Human Rights Law
STUDENT'S NAME: Mitchell E Paquette
SUPERVISORS'S NAME: Stephen J Malby
DISSERTATION TITLE **"The Human Rights Impact of Technology Sanctions"**

COMMENTS: (PLEASE WRITE BELOW YOUR COMMENTS)

MARK:	
SIGNATURE:	**DATE:**

UNIVERSITY OF ESSEX

SCHOOL OF LAW

LLM/MA in International Human Rights Law

2018-2019

Supervisor: Steven Malby

DISSERTATION

The Human Rights Impact of Technology Sanctions

Name: Mitchell E Paquette
Registration Number (optional):1802326
Number of Words: 19,989
Date Submitted: 03/10/2019

1. Introduction

Since the 1990s, when economic sanctions imposed by the United Nations (UN) on Iraq reportedly resulted in up to 227,000 deaths caused by skyrocketing food prices and limited medical supplies,[1] the international community has been more attuned to the possible negative impacts that such measures might have on human rights in the targeted state.[2] In 2014, the the UN Human Rights Council (HRC) reaffirmed that 'essential goods, such as food and medicines, should not be used as tools for political coercion and that under no circumstances should people be deprived of their own means of subsistence and development.'[3] However, as global societies and economies have evolved, so too have the nature of sanctions regimes and their effects. Increasingly, sanctions regimes imposed by states and international organizations, led by the UN, the European Union (EU) and the United States (US), specifically restrict the transfer of technological goods and services, which might be used by the targeted regime in weapons development, surveillance, or cyberwarfare.[4] Only in the past decade has it been considered that many of these very same tools and services also have tremendous positive effects on the exercise of human rights in the targeted state, used by citizens as a means of communication, accessing information, and otherwise engaging with the global economy of information and communication technologies (ICTs).[5]

This issue gained recognition in the context of US-imposed sanctions during the 2009 Iranian Green Movement and the Arab Spring, when ICTs including platforms like Twitter, Facebook, and Telegram played a pivotal role in civil society organizing against repressive governments,[6] despite sophisticated state-sponsored surveillance and censorship programs.[7] The international community soon realized the importance of ICTs for sharing information, communication, and evading government censors and

[1] A/HRC/39/54, para 34
[2] Dursun Peksen, "Better or Worse? The Effect of Economic Sanctions on Human Rights," (Journal of Peace Research, 46(1) 2009), p. 59; see also David Cortright and George Lopez, "Smart sanctions: targeting economic statecraft," (Rowman & Littlefield, 2002)
[3] A/HRC/RES/27/21, para 9
[4] Pinky P. Mehta, "Sanctioning freedoms: U.S. sanctions against Iran affecting information and technology companies," (UPJIL, 37(2) 2016), p. 768
[5] Danielle Kehl, Tim Maurer, & Sonia Phene, "Translating Norms to the Digital Age: Technology and the Free Flow of Information under U.S. Sanctions," (NEW AM. FOUND., 4 Dec. 2013), p. 2
[6] Mehta, p. 765
[7] Peter Harrell and Collin Anderson, "U.S. Sanctions Abet Iranian Internet Censorship," (Foreign Policy, January 22, 2018)

surveillance, as well as the severe impact that sanctions had on access to these tools.[8] The US State Department acknowledged this reality in a formal statement, recognizing that 'Over the last several years, the world has witnessed the important role this technology can assume in holding repressive regimes accountable, assisting people in exercising their human rights and protecting emerging elements of civil society.'[9] Accordingly, the US took steps to amend sanctions policies by providing exemptions for certain technologies across active sanctions regimes in Cuba, Syria, Sudan, and Iran.[10]

However, many claim that these measures have had little effect on the accessibility of US-sourced technologies in the targeted states,[11] in part due to 'overcompliance' on the part of companies subject to these export restrictions, either because of a lack of clarity around sanctions policies or overly cautious approaches to compliance.[12] The impact on human rights as a consequence of continued sanctions-related restrictions on access to technology has reportedly been substantial and broad in scope. For example, after a 2018 country visit to Syria, the UN Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, Idriss Jazairy, reported that US sanctions prohibited the export of 'almost all electronic goods, including computers and mobile smartphones with American processors or software,' and had affected nearly all sectors of the economy.[13] After a similar visit to Sudan, the Special Rapporteur reported that the lack of technical support and equipment due to US sanctions left medical professionals struggling to conduct effective medical diagnostics and deprived students of software and technology which would improve their learning.[14] As one expert described in the context of Iran, prior to the issuing of general licenses in 2010, sanctions on technology exports were so broad that they 'could encompass everything developed in the computer age.'[15]

[8] Kehl et al, p. 2
[9] U.S. Dep't of State, Pub. Notice 8086, State Department Sanctions Information and Guidance (Nov. 8, 2012).
[10] U.S. Dep't of Treas., General License Related to Personal Communication Services (2010); U.S. Dep't of Treas., General License D-1 with Respect to Certain Services, Software, and Hardware Incident to Personal Communications (2014).
[11] Elias Groll, "Why US sanctions are actually helping Iran crack down on protesters," (Foreign Policy, Jan 7, 2018)
[12] Mehta, p. 778; see also A/HRC/39/54/Add.2, para 37
[13] A/HRC/39/54/Add.2, para 47
[14] A/HRC/33/48/Add.1, para 25
[15] Vahe Petrossian, "Iran Back in the Firing Line," 36 MIDDLE E. ECON. DIG. 2, 2 (Dec. 4, 1992)

As such, it is clear that restrictions on technology can have broad effects on the targeted state's population, which have serious implications for the protection of many fundamental human rights.[16] Nevertheless, economic sanctions continue to be a regular feature of modern foreign policy with 14 active sanctions regimes currently implemented by the UN Security Council,[17] and more than 30 separate unilateral sanctions regimes imposed by the US and EU respectively.[18] With cyber operations including surveillance, online censorship, and state-sponsored hacking emerging as an increasingly common feature of both internal and external modern conflicts,[19] it is reasonable to assume that technology will continue to play an important role in future sanctions regimes. Thus far, efforts to address this matter have typically approached it from the perspective of policy,[20] however, given the above-stated effects and their potential impact on human rights, this essay seeks examine whether states might be held legally responsible under the international human rights law framework for violations related to the impact of technology sanctions.

Applying a human rights law framework to this matter presents a number of challenges and involves a convergence of multiple areas of legal uncertainty. For one, whereas human rights have typically been understood as legal obligations owed by a state to its citizens,[21] the matter of sanctions deals with the relationship between the human rights obligations of a state imposing sanctions with respect to the impact of its policies on the population of another, otherwise known as extraterritorial obligations.[22] The nature of such obligations is subject to endless debate amongst legal scholars and inconsistent jurisprudence within and across human rights courts.[23] Further, considering that the human rights framework was developed before many modern technologies and their implications for individual rights could have been imagined,

[16] Dursun Peksen. & A. Cooper Drury, "Economic Sanctions and Political Repression: Assessing the Impact of Coercive Diplomacy on Political Freedoms," (Hum Rights Rev, Vol. 10, Issue 3, 2009)
[17] UN DPPA Fact Sheets, "Subsidiary Organs of the United Nations Security Council," (8 February 2019).
[18] European Parliament, "EU sanctions: A key foreign and security policy instrument," (May 2018) and U.S. Dept. of Treasury, "Sanctions Programs and Country Information".
[19] Giovanni Ziccardi, *Resistance, Liberation Technology and Human Rights in the Digital Age*, (Springer Netherlands, 2013), ch. 6.
[20] see Mehta and Kehl et al.
[21] Malcolm Langford et al (eds.), *Global Justice, State Duties: The Extraterritorial Scope of Economic, Social, and Cultural Rights in International Law*, (CUP, 2012), p. 3
[22] The Special Rapporteur on the negative impact of unilateral coercive measures has raised as an unresolved matter whether 'States (or international organizations) are subject to extraterritorial obligations under human rights instruments in relation to the application and effects of sanctions;' see A/HRC/36/44, para 20
[23] see Marko Milanovic*, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy*, (OUP, 2011)

and despite efforts within the UN to bring understandings of human rights obligations up to date with the digital age, the scope and content of human rights with respect to modern technology is not well-established.[24]

The following analysis will thus seek to address each of these matters in turn, drawing on the existing human rights law framework and applying it to the effects of technology sanctions. Chapter 2 will first address the issue of extraterritorial obligations under the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR), as well the human rights responsibilities applicable to multinational corporations given their role in implementing sanctions. Chapter 3 will then consider the effects of technology sanctions, focusing on US sanctions in Iran, Syria, and Sudan as these are the most well-documented case studies available,[25] with regard to the content of the implicated rights contained in both the ICCPR and ICESCR. It will then evaluate these effects in light of the legal obligations and models of extraterritorial jurisdiction identified in chapter 2, in order to assess whether such effects could amount to violation of a state or international organization's human rights obligations.

2. Extent of Legal Obligations

2.1 Scope of Human Rights Obligations

The human rights legal framework primarily consists of the fundamental norms established by the Universal Declaration of Human Rights (UDHR), the ICCPR and its two optional protocols, and ICESCR. Both the ICCPR and ICESCR establish obligations which state parties to the treaties are legally bound to respect, protect, and fulfil, and together with customary international human rights obligations form the foundation of the international human rights law framework.[26] Other instruments have been adopted at the regional level, as have more specialized international treaties, however, the scope of this paper will focus

[24] Jacopo Coccoli, "The Challenges of New Technologies in the Implementation of Human Rights: an Analysis of Some Critical Issues in the Digital Era," (Peace Human Rights Governance, 2017), p. 229

[25] As this analysis focuses on international human rights law, any conclusions drawn with respect to US sanctions would generally apply to similar sanctions regimes imposed by other states or international organizations

[26] Frédéric Mégret, "Nature of Obligations," in Moeckli et al. (eds) *International human rights* law (3rd edn. OUP 2014)

on the legal obligations established under ICCPR and ICESCR, to which the vast majority of states are party to.[27]

While the content of the specific rights affected by technology sanctions will be discussed alongside the human rights impact of such measures in chapter 3, this chapter primarily focuses on the general legal obligations set out in the treaties, namely which individuals states owe human rights obligations to. In all cases, determining a violation of international legal obligations rests on whether specific conduct may be attributed to the State and whether or not that conduct constitutes a breach of the obligations owed by the State.[28] However, international human rights treaties like the ICCPR and the European Convention on Human Rights (ECHR) uniquely introduce one-way obligations owed to certain individuals 'subject to the degree of attachment' between the individual and the contracting state.[29] Thus, a third determining factor arises in the context of human rights violations, typically defined as one of 'jurisdiction.'[30] While this requirement has led to the dominant understanding of human rights obligations as something owed by the state to its own citizens, there is growing recognition that human rights law may also apply extraterritorially.[31] However, as the UN General Assembly recognized in 2017, 'the scope of such obligations remains a matter of contention.'[32] This chapter will consider the current models and debates regarding extraterritorial jurisdiction with respect to the ICCPR and ICESCR, as well as the emerging understanding of human rights duties and obligations as they apply to corporate non-state actors.

2.1.1 Civil and Political Rights

[27] While the US has only signed but not ratified ICESCR, some aspects of the treaty are now recognized as customary international law binding on all states. Further, under article 18(a) of the Vienna Convention on the Law of Treaties (1969), as a signatory the US is obligated not to take actions that would defeat the 'object and purpose' of the treaty; see Margot E. Salomon, "Deprivation, Causation and the Law of Intl Cooperation," in Langford et al (eds), p. 270

[28] "Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission on the Work of Its Fifty-third Session," UN GAOR, 56th Sess., Supp. No. 10, at 43, UN Doc. A/56/10 (2001), Article 1

[29] Maarten den Heijer and Rick Lawson, "Extraterritorial Human Rights and the Concept of 'Jurisdiction'" in, Langford et al (eds), p. 158

[30] Martin Scheinin, "Just Another word? Jurisdiction in the Roadmaps of State Responsibility and Human Rights," in Langford et al (eds)

[31] see Mark Gibney and Sigrun Skogly, *Universal human rights and extraterritorial obligations*, (University of Pennsylvania Press, 2010)

[32] GA A/72/370 (2017), para 34

Human rights treaties define their scope of application differently on the basis of 'jurisdiction'[33] and 'territory.'[34] While some human rights treaties contain no mention of 'jurisdiction,' such as the ICESCR discussed later in this chapter, and thus might be interpreted more broadly, others such as the ICCPR and ECHR[35] are more limited. Article 2(1) of the ICCPR requires States 'to respect and to ensure [rights] to all individuals within its territory *and* subject to its jurisdiction.' The most widely adopted[36] reading of this provision, articulated in HRC General Comment 31, holds that States owe rights to all persons 'within their territory' and to all persons 'subject to their jurisdiction,' meaning that 'a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State Party.'[37] However, the HRC has also stated that 'it would be unconscionable to so interpret the responsibility under article 2 of the Covenant on Civil and Political Rights as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory.'[38] This opinion is cited by Jazairy as grounds for the existence of extraterritorial obligations with respect to States enacting unilateral sanction,[39] although it is questionable whether this is supported by existing models of extraterritorial obligations established through international jurisprudence.

Extraterritorial obligations were first discussed by human rights courts in relation to State occupation of foreign territory. The *Loizidou*[40] case, concerning Turkey's occupation of Northern Cyprus, was the first to establish jurisdiction on the basis of 'effective control,' asserting that jurisdiction is not derived from a State's mere presence in a foreign territory, but rather the level of control exerted within it.[41] Thus, states have extraterritorial human rights obligations with respect to any individual located within a territory under its

[33] Some treaties, such as the International Covenant on Economic, Social, and Cultural Rights (ICESCR), contain no mention of 'jurisdiction' and thus might apply more broadly; see note 29, p. 159
[34] Olivier de Schutter, *International Human Rights Law: Cases, Materials, Commentary* (2nd edn, CUP 2014), p. 147
[35] Under ECHR Art. 1, States owe the treaty rights 'to everyone within their jurisdiction'
[36] The United States and Israel adopt a conjunctive reading which rules out the extraterritorial application of ICCPR; see Ashley Deeks, "Does the ICCPR Establish an Extraterritorial Right to Privacy?" *Lawfare*, (14 Nov 2013)
[37] HRC General Comment 31, CCPR/C/21/Rev.1/Add.13, para 10
[38] A/36/40, *Sergio Euben Lopez-Burgos v. Uruguay*, communication no. R.12/52, para. 12.3.
[39] A/70/345 (2015), para 14
[40] *Loizidou v. Turkey* (Judgment), App. No. 15318/89, 310 Eur. Ct. H.R. (1995), para. 62
[41] Milanovic, p. 118

effective control (spatial model).[42] However, jurisdiction has also been defined with respect to power or effective control over individuals (personal model)[43] such as in the Human Rights Committee's ruling in *Lopez-Burgos v. Uruguay*, which held that 'jurisdiction' does not necessarily refer to the territory in which the violation occurred, 'but rather to the relationship between the individual and the State.'[44]

The European Court of Human Rights' (ECtHR) decision in *Bankovic v Belgium*[45] rejected major aspects of the *Lopez-Burgos* decision, holding that not every exercise of authority affecting a person's enjoyment of human rights brings that person under a State's jurisdiction and reasserting the notion that jurisdiction is primarily territorial.[46] However, the *Bankovic* decision was largely reversed by a later ECtHR judgement in *Al-Skeini and Others v. UK*, a detention case in which the Court recognized both 'control and authority' by a state agent and 'effective control' of territory as constitutive of extraterritorial jurisdiction, and asserted a 'divided and tailored' approach to rights obligations.[47] Under this view, extraterritorial obligations are contextual such that control over the individual does not necessarily give rise to the full spectrum of human rights obligations, but only those relevant to the given situation. This conception has been further expanded to include situations where a State does not physically detain an individual but still exercises authority and control over them, such as within a vehicle checkpoint[48] or in the case of *Pad v Turkey*, where the ECtHR found that Turkey exercised jurisdiction over the right to life of victims killed by gunfire from a helicopter.[49]

Earlier models of extraterritorial jurisdiction based on effective control and state agent authority and control would likely not apply to the situation of human rights interferences resulting from economic sanctions, given that the effects of sanctions do not depend on the sanctioning state exercising physical presence or effective control within the targeted state.[50] However, more recent jurisprudence[51] suggests

[42] see *Advisory Opinion Concerning Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* International Court of Justice (ICJ), 9 July *2004*, para 109
[43] see HRC General Comment 31, para 10
[44] *Lopez-Burgos v. Uruguay,* paras 12.2–12.3
[45] *Bankovic et al. v. 17 NATO Member States* App no. 52207/99 (ECtHR, 12 December 2001)
[46] Milanvoic, p. 118
[47] *Al-Skeini v. Sec'y of State for Def. (Judgement),* App. No. 55721/07, 2011 Eur. Ct. H.R., para 79; see also *Öcalan v. Turkey [GC],* no. 46221/99, § 91, ECHR 2005-IV
[48] *Jaloud v the Netherlands*, App. No. 47708/08, 2014
[49] *Pad and Others v Turkey*, App. No. 60167/00, 2007
[50] GA A/72/370, para 44
[51] see note 48 and 49

that exercising control and authority over an individual's *rights*, regardless of physical proximity or territorial control, is sufficient grounds for finding extraterritorial obligations with respect to those rights. Such cases lend some validity to a third model of jurisdiction, referred to as the 'impact model,' described by legal scholar Marko Milanovic.[52] Drawing on the notion that rights may be 'divided and tailored' based on the level of control exerted, Milanovic argues that a state's obligation to respect human rights, which does not depend on control over an area, should be territorially unbound and incurred whenever a state has an impact on an individual's rights extraterritorially.[53] In General Comment 36, the HRC seems to articulate a similar understanding, asserting that states have an obligation to 'respect and ensure' rights to 'all persons over whose enjoyment of the right to life it *exercises power or effective control*.'[54] It further specifies that this 'includes persons located outside any territory effectively controlled by the State, whose right to life is nonetheless *impacted* by its military or other activities in a *direct and foreseeable* manner.'[55] While some states objected to this formulation of extraterritorial obligations, which is not entirely supported by existing jurisprudence, legal scholars have argued that it would address many of the existing inconsistencies in the established practice of the HRC and ECtHR with respect to extraterritorial obligations.[56] Applied in the context of technology sanctions, it seems a more promising approach for establishing extraterritorial obligations for the sanctioning state on the basis that by restricting access to certain ICT tools, the state exercises power over the rights implicated in the use of ICTs, such as the right to freedom of expression, despite having no physical presence or effective control in the targeted state.

2.1.2 Economic, Social and Cultural Rights

As shown above, the typical approach to extraterritoriality with respect to civil and political rights has largely centered on the degree to which territory and jurisdiction limit the scope of state obligations.[57] The same does not hold true for economic, social and cultural (ESC) rights given that article 2(1) of the

[52] Milanovic, p. 209
[53] ibid, p. 211
[54] CCPR/C/GC/36, para 63; see also Concluding Observations: United Kingdom (2008), para. 14
[55] General Comment 36, para 63; see also Concluding Observations: USA (2014), para. 9
[56] Daniel Møgster, "Towards Universality: Activities Impacting the Enjoyment of the Right to Life and the Extraterritorial Application of the ICCPR," (EJIL Talk!, 27 Nov 2018)
[57] Langford et al, p. 6

ICESCR, which defines the scope of the treaty obligations, makes no reference to 'jurisdiction' or 'territory' and includes an obligation that state parties 'take steps, individually and through international assistance and co-operation,' to progressively realize ESC rights.[58] In the absence of explicit jurisdictional limitations, debate has instead surrounded whether the ICESCR establishes legally binding extraterritorial obligations, with many Western states asserting that it imposes only moral rather than legal obligations.[59] This position is becoming less tenable, as there is emerging consensus about the customary law nature of economic, social and cultural rights (particularly minimum core obligations) [60] as well as at least a negative extraterritorial obligation to respect ESC rights when a state's actions have an impact outside of their territory,[61] although no case law has yet dealt with this matter explicitly.[62]

While the ICESCR makes no explicit mention of jurisdiction, there are strong indications that some basis of jurisdiction must be satisfied for a violation to be attributed to a State.[63] The Maastricht Guidelines on Violations of Economic, Social and Cultural Rights for example hold that violations are 'imputable to the State within whose jurisdiction they occur,'[64] and the ICJ asserted generally in *DRC v Uganda* that 'international human rights instruments are applicable in respect of acts done by a state *in the exercise of its jurisdiction* outside its own territory.'[65] Further, the Optional Protocol establishing an individual complaint mechanism for ICESCR introduces as an admissibility condition that the applicant be 'under the jurisdiction' of the State Party that the complaint is filed against.[66] Two primary bases of extraterritorial jurisdiction have emerged with respect to ESC rights and could be applied in accounting for the extraterritorial human rights impact of technology sanctions: 1) a model based on the effective control test and 2) a model based on the general obligation to provide 'international assistance and co-operation.'[67] Although the effective control

[58] A/HRC/36/44 (2017), para 34
[59] Olivier De Schutter et al, 'Commentary to the Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights' (2012) 34 Human Rights Quarterly, p. 1094
[60] CESCR General Comment 3, para 10
[61] Langford et al, p. 112
[62] see *Threat or use of nuclear weapons*, ICJ Reports, 1996 (Advisory Opinion) and ICJ *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, para 112 for some legal basis
[63] Langford et al, p. 60
[64] International Commission of Jurists (ICJ), Maastricht Guidelines on Violations of Economic, Social and Cultural Rights, 26 January 1997, para 16
[65] *Case Concerning Armed Activities on the Territory of the Congo* (Democratic Republic of the Congo v. Uganda), ICJ, Judgement, 19 December 2005, para 216
[66] CESCR Optional Protocol, art. 2
[67] Langford et al (eds), p. 61

model has typically been applied to civil and political rights, given the interrelated and interdependent nature of international human rights, it is suggested that the same threshold may also apply to ICESCR obligations.[68] However, considering that most extraterritorial violations of ESC rights are unlikely to satisfy the high threshold that the effective control standard imposes,[69] including violations related to economic sanctions, its application would be extremely limited and a less restrictive basis for establishing extraterritorial state obligations is likely required.[70]

In the absence of any specific jurisdictional limitations under the general legal obligations of ICESCR and considering the obligation to provide 'international assistance and cooperation'[71] towards the full realization of ESC rights, it could be interpreted that State parties assume legal obligations with respect to ESC rights that are international or extraterritorial in scope. In the absence of any relevant jurisprudence on the matter, the Maastricht Principles on Extraterritorial Obligations of States in the area of Economic, Social and Cultural Rights describe three separate situations amounting to extraterritorial jurisdiction under ICESCR.[72] In addition to the aforementioned situation of effective control or authority, the Maastricht Principles assert that states have obligations with respect to acts or omissions that 'bring about *foreseeable* effects on the enjoyment of ESC rights' within or outside of its territory, even in the absence of effective control or authority over a situation or person.[73] Lastly, the Maastricht Principles assert that a state may have extraterritorial obligations when it is in a position to 'exercise decisive influence or to take measures to realize ESC extraterritorially,[74] suggesting that states may also incur positive extraterritorial obligations under certain circumstances.

[68] Narula, p. 123

[69] Some have proposed a standard based on 'effective economic control' to account for situations in which a state exercising control over economic policies or markets impacts human rights in a foreign state; see Smita Narula, "International Financial Institutions, Transnational Corporations," in Langford et al (eds), p. 125

[70] Langford et al, p. 8

[71] CESCR General Comment 3, para 14 asserts that this is a legal obligation of all state parties; see also Article 56 of the UN Charter and Part I, paragraph 34 of the Vienna Declaration and Programme of Action

[72] Although the Maastricht Principles are not legally binding, they still carry the authority of significant legal expertise in the area of ESC rights; see Maastricht Principles on Extraterritorial Obligations of States in the area of Economic, Social and Cultural Rights, Principle 9

[73] This would be consistent with the 'causation model' in Chapter 2.1.3; see Maastricht Principles, Art. 9(b) and De Schutter et al, p. 1109

[74] Maastricht Principles, Principle 9(c)

As to the nature of these extraterritorial obligations, the Maastricht Principles assert that states have obligations to respect, protect, and fulfill ESC rights extraterritorially.[75] This is in accordance with CESCR's position on the matter expressed in relation to multiple rights, such as General Comment 12 on the right to food which stresses the 'essential role of international cooperation' and that 'State Parties should take steps to respect the enjoyment of the right to food in other countries, to protect that right, to facilitate access to food and to provide the necessary aid when required.'[76] Thus, states may have both negative and positive extraterritorial obligations under the ICESCR. Legal scholars have sometimes proposed a graduated approach to the scope of obligations, contingent on the degree of control exercised by the State in another territory.[77] Given the lack of proximity and control in most cases between a sanctioning state and the target state, it is unlikely that there would be strong legal grounds for asserting an obligation to fulfill rights in the target state. Thus, the obligations of the sanctioning state would be limited to the obligation to respect and protect[78] ESC rights.

Stemming from the obligation of international cooperation, CESCR has clarified that the obligation to respect rights extraterritorially 'requires States parties to refrain from interfering directly or indirectly with the enjoyment of the Covenant rights by persons outside their territories.'[79] This coincides with the obligation under the Maastricht Principles that States *must* 'desist from acts and omissions that create a real risk of nullifying or impairing the enjoyment' of ESC rights extraterritorially, and that state responsibility is incurred whenever 'such nullification or impairment is a foreseeable result of their conduct.'[80] The Maastricht Principles further distinguish between direct and indirect interference under the obligation to respect ESC rights. Direct influence refers to situations where the conduct of the state has potential impact on the enjoyment of ESC rights 'without the involvement of any other state or international organization.'[81] Indirect influence refers to conduct which 'impairs the ability of another State or international organization to comply'

[75] Maastricht Principles, Principle 3
[76] CESCR General Comment 12, para 36
[77] Langford et al, p. 61
[78] discussed in chapter 2.2
[79] E/C.12/GC/24, para. 29; see also E/C.12/2002/11, para. 31
[80] Maastricht Principles, Principle 13
[81] ibid, Principle 20

with its own ESC rights obligations.[82] The latter has obvious applicability for detrimental rights impacts stemming from economic sanctions and the enforced deprivation of certain goods or services.

Recognizing the particular relevance of economic sanctions in the context of extraterritorial ESC rights obligations, the Maastricht Principles specifically address the duties of sanctioning states under the obligation to respect human rights. Principle 22 asserts that States must refrain from adopting sanctions which would nullify or impair 'the enjoyment of economic social and cultural rights,' especially those affecting 'goods and services essential to meet core obligations.' This position is consistent with CESCR General Comment 8, which sets out certain obligations of 'parties responsible for the imposition, maintenance or implementation of the sanctions, whether it be the international community, an international or regional organization, or a State or group of States.'[83] This includes the obligation to ensure that the measures imposed do not cause 'disproportionate suffering' within the targeted country and that any negative impact on human rights is limited to the greatest extent possible.[84] In accordance with these obligations, some argue that states or other organizations must terminate sanctions if their negative impact on human rights outweighs the objective being sought.[85]

A more recent source of guidelines regarding the extraterritorial application of ESC rights with respect to economic sanctions comes from the 2017 report by Special Rapporteur Idriss Jazairy. Although Jazairy acknowledges ongoing debates over the extraterritorial application of ICESCR obligations, he concludes that sanctions should fall within the ambit of situations that incur extraterritorial obligations, even when the sanctioning state exercises no formal jurisdiction or control over the affected population.[86] In an annex to the 2017 report outlaying 'Elements for a draft General Assembly declaration on unilateral coercive measures and the rule of law,' Jazairy asserts far-reaching extraterritorial obligations for sanctioning states such that 'in situations where unilateral coercive measures inflict undue sufferings/have an egregious human rights impact, on the population of a targeted State…they become clearly illegal and their source countries should be called to account.'[87] While such a position may have limited support in existing

[82] Maastricht Principles, Principle 21
[83] CESCR General Comment 8, E/C.12/1997/8, para 11
[84] GC 8, para 14; see also De Schutter et al, p. 1132
[85] De Schutter et al, p. 1133
[86] A/HRC/36/44, para 33 and 52
[87] A/HRC/36/44, Annex I, para 7

jurisprudence, the statement clearly suggests that in the opinion of the Special Rapporteur, any unilateral sanction which has substantial adverse impacts on human rights is unlawful and should lead to state responsibility.

2.1.3 Causation Model

In support of a more flexible approach to extraterritorial jurisdiction, which may be required to address the impact of policies like economic sanctions, Jazairy suggests an approach based on causality[88] whereby "whether a technical exercise of jurisdiction or not, the type of act instituted by the State will essentially dictate who is affected, who falls within its jurisdiction, the rights violated and the extent of obligations owed."[89] The principle of causality is related to state responsibility, which is determined by whether, based on the facts of a situation, an outcome amounts to a human rights violation that can be causally linked to the acts or omissions of a state (factual causality) *and* whether under the relevant legal requirements such unlawful acts or omissions are attributable to the state.[90] Under international human rights law, this latter requirement has typically carried a high threshold of jurisdiction such as overall or effective control,[91] and thus extraterritorial responsibility has been difficult to establish.[92] However, as Sigrun Skogly points out, this leads to a discrepancy between factual causation and attribution, which allows those who factually carried out the act or omission to avoid legal responsibility.[93] Thus, a revised approach to State responsibility more closely linked to factual causality may be necessary.[94]

Principles of 'foreseeability' and 'proximity' have been used in other contexts to establish the scope of responsibility for an internationally wrongful act when factual causality can be established,[95] and some have suggested that these principles could also be applied under international human rights law.[96] Proximity is

[88] A/72/370, para 42
[89] Eleni Kannis, Pulling (Apart) the Triggers of Extraterritorial Jurisdiction, 40 U.W. AUSTL. L. REV. 221, 243 (2015), p. 234
[90] ILC Articles on State Responsibility, Chapter II
[91] See *Bankovic*, and *Wall advisory opinion*
[92] Sigrun I. Skogly, "Causality and Extraterritorial Human Rights Obligations," in Langford et al., p. 243
[93] ibid
[94] The ECtHR has cautioned against such a "cause-and-effect" notion of jurisdiction; see *Bankovic*, para 75
[95] Skogly, p. 244
[96] see CCPR/C/96/D/1539/2006, Communication No. 1539/2006 (Munaf v. Rom.) in which the HRC affirms that a state may be held legally responsible for extraterritorial violations when the violation is a 'necessary and

related to the degree to which a harm is directly related to the actions of a state[97] while foreseeability refers to whether a State knew or should have known that its acts or omissions would result in substantial human rights impacts extraterritorially or failed to undertake adequate due diligence to prevent or mitigate a violation.[98] Perhaps the clearest example of how state responsibility for extraterritorial human rights impact could be evaluated on this basis comes from the Inter-American Court of Human Rights (IACtHR) Advisory Opinion OC-23/17, in which the Court addressed whether a state party could be held legally responsible for extraterritorial human rights violations caused by 'serious' or 'significant' environmental impact attributable to it.[99] In its decision, the Court recognized that a person may come under the jurisdiction of a state 'if there is a *causal link* between the action that occurred within its territory and the negative impact on the human rights of persons outside its territory,'[100] such that the state 'exercises effective control *over the activities* that caused the damage.'[101] It further suggests that 'effective control' in this context would be evaluated on the basis of proximity and foreseeability,[102] subject to whether a state had knowledge of the risk of wrongful acts and the capacity to protect against such effects.[103] However, the Advisory Opinion has been criticized for its lack of clarity around the minimum threshold of 'seriousness' of the damage for extraterritorial jurisdiction to be incurred, as well as the precise criteria for establishing a 'causal link.'[104] Despite this criticism, and while the approach of a regional court of human rights does not have universal applicability across other human rights bodies, the IACtHR's more flexible approach to jurisdiction could have implications for future considerations of extraterritorial jurisdiction under both the ICCPR and ICESCR which would greatly increase the likelihood of finding State responsibility for the negative human rights impact of sanctions.

2.2 Non-State Actors

foreseeable' consequence of its actions; see also James Crawford, *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries* (CUP, 2002), p. 204

[97] De Schutter et al, p. 1109

[98] ibid, p. 1113

[99] IACtHR Advisory Opinion OC-23/17, NOV 15, 2017, para 136

[100] ibid, para 104(h)

[101] ibid, para 102 and 104(h)

[102] ibid, para 136

[103] Antal Berkes, "A New Extraterritorial Jurisdictional Link Recognised by the IACtHR," EJIL: Talk! (March 28, 2018)

[104] ibid

While the above frameworks on extraterritorial jurisdiction may provide a route to state responsibility for the negative human rights impact of sanctions (technology-related or otherwise), it must not be forgotten that the effects of sanctions may not be the direct result of sanctions policies themselves, but rather the decisions of companies to restrict the transfer of certain goods or services *in reaction* to the sanctions.[105] Thus, the relationship between the state and private actors under its jurisdiction, as well the actions of companies independent of the state, merit consideration when attempting to establish accountability. It is particularly relevant in the case of technology sanctions given the problem of overcompliance described in chapter 1, where companies under the jurisdiction of the sanctioning state, as well as those who do not wish to jeopardize their economic activities with said state, deny products and services to the targeted state beyond what the sanctions regime would otherwise require.[106]

There are a number of reasons why companies engage in overcompliance, including reputational concerns of doing business with governments targeted by sanctions[107] and substantial financial and legal penalties for sanctions infringements.[108] However, blame for the practice of overcompliance does not solely rest with the companies themselves. The sanctions regimes that States create for businesses to follow are often vague, complex, and subject to frequent changes, leaving significant ambiguity over what products and services can and cannot be legally exported to the targeted state.[109] Thus, companies often take a 'risk-averse approach' and refrain from providing products or services in the targeted State until they receive 'explicit authorization in the form of interpretive guidance or specific licenses.'[110] As such, addressing the problem of overcompliance depends on companies ensuring that they are carrying out lawful business activities while not restricting access to vital services and technologies unnecessarily, as well as States designing clearer sanctions regimes and exemptions which produce greater legal certainty for companies to operate under.

While states carry duties with respect to companies under their jurisdiction under the obligation to protect human rights, companies themselves are not traditionally considered subjects of international law

[105] Ali Bangi, "The Impact of Sanctions Overcompliance on Iran," (Iran Cyber Dialogue, 28 March 2016)
[106] A/HRC/36/44 (2017), para 27
[107] Mehta, p. 782
[108] Elias Groll, "Why US sanctions are actually helping Iran crack down on protesters," (Foreign Policy Jan 7, 2018)
[109] Mehta, 781
[110] Kehl et al, p. 18

and thus must be regulated via the state.[111] However, there is growing recognition that companies carry a *responsibility* to respect human rights, most clearly articulated in the UN Guiding Principles on Business and Human Rights.[112] While the authority of the Guiding Principles is limited to that of a soft law initiative and thus not binding on states, it is asserted that its three pillar framework is reflective of existing international legal standards and obligations for states and businesses.[113] Further, the Guiding Principles have been unanimously endorsed by the UN HRC and incorporated into numerous international regulatory frameworks around corporate accountability for human rights violations.[114]

Although not completely voluntary, the responsibility of corporate actors to respect human rights is softer than the obligation on States to protect human rights. It provides that businesses should refrain from infringing on human rights and address adverse impacts linked to their activities through prevention, mitigation, and remediation.[115] The primary duty described is that of carrying out effective due diligence to identify and address negative human rights impacts, which would include assessments of what products are subject to export restrictions such as sanctions.[116] The extent of the responsibility varies based on the size and capacity of the enterprise and should be conducted continuously throughout a business' operations.[117] Effective due diligence is necessary for business enterprises to avoid complicity in human rights abuses committed by other parties, which could carry liability for civil or criminal wrongs.[118] When adverse human rights impacts are identified in connection with a business enterprise's activities, the appropriate action that it should take varies according to the nature of its contribution to it and the amount of leverage it can exercise in addressing the impact.[119] Thus, in evaluating the responsibilities of corporate actors in the context of sanctions, they should be understood as variable with respect to their level of

[111] Narula, p. 139
[112] 'Guiding Principles on Business and Human Rights: Implementing the United Nations' "Protect, Respect and Remedy" Framework,' UN Doc. A/HRC/17/31 (21 March 2011).
[113] ibid
[114] Jonathan Bonnitcha and Robert McCorquodale, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights," *European Journal of International Law*, (Vol. 28, Issue 3, Aug 2017), p. 900
[115] UNGPs, Principle 11 and 13
[116] see Bonnitcha and McCorquodale, p. 900
[117] UNGPs, Principle 17(b) and (c)
[118] UNGPs, Principle 17 Commentary
[119] UNGPs, Principle 19(b)

connection to the adverse human rights impacts of their activities, but at a minimum, amount to effective due diligence when making decisions about how to comply with such measures.

In addition to the responsibilities of companies, the first pillar of the UN Guiding Principles framework pertains to the duty of States to protect against human rights violations carried out by private actors under their jurisdiction or within their territory through effective legislation. States are obligated to ensure that laws and policies governing the business sector 'do not constrain but enable business respect for human rights,' and 'provide effective guidance' to businesses on how to respect human rights.[120] The Commentary to this principle also asserts that States have a duty to review whether the laws governing business enterprises 'provide the necessary coverage in light of evolving circumstances and whether…they provide an environment conducive to business respect for human rights.'[121] Thus, it would seem that based on this framework, States in designing sanctions and coercive measures have a duty to ensure that such policies enable businesses to carry out their duty to respect human rights, to provide guidance on compliance to businesses operating under the sanctions regime, and to revise such sanctions when necessary. This duty to protect would also extend to states acting as members of multilateral institutions.[122]

Under the obligation to protect against abuses carried out by non-state actors, while it is asserted that States are not *directly* responsible for the abuses of third parties,[123] their acts may be indirectly attributable[124] to the State when it fails to take the required steps to 'prevent, investigate, punish and redress' such abuses.[125] Thus, indirect attribution of extraterritorial human rights violations would be based on whether the state conducted appropriate due diligence to avoid foreseeable violations by non-state actors, proportionate to its capacity to influence the corporations implicated.[126] Vassilis Tzevelekos suggests that standards of due diligence might also be dependent on and proportional to the effectiveness

[120] UNGPs, Principle 3
[121] ibid, 'Commentary'
[122] UNGPs, Principle 10
[123] UNGPs, 'Foundational Principles'
[124] Vassilis Tzevelekos, "Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct Attribution of Wrongfulness, Due Diligence, and Concurrent Responsibility" (MJIL, Vol. 36:129, 2014), p. 152
[125] UNGPs, 'Foundational Principles'
[126] see *Velasquez Rodriguez v Honduras*, IACtHR Judgement, 29 July 1989, 28 ILM 291, para 172; see also Maastricht Guidelines, Guideline 18

of the control exerted by the state over a particular situation.[127] While many aspects of this argument for the indirect attribution of *extraterritorial* breaches of human rights to the host state remain unclear and untested, there appears to be emerging consensus amongst legal scholars that such an obligation is included under a state's positive extraterritorial obligation to protect human rights.[128] Applied in the context of technology sanctions, this approach offers a solid basis for establishing state responsibility when private actors, in complying with such sanctions, infringe on the rights of individuals in the targeted state. Due diligence in this scenario might amount to issuing general licenses, revising or providing greater clarity on sanctions policies, or directly regulating the actions of private actors under the state's jurisdiction to ensure that their sanctions regimes do not lead to infringements on human rights.[129]

3. Legal Analysis

As demonstrated above, there are a number of challenges in applying the existing international human rights law framework to the matter of sanctions. The current understanding and existing jurisprudence surrounding extraterritorial human rights obligations, the lack of clarity around the scope of ESC rights, specifically the nature of the obligation of 'international cooperation and assistance,' as well as the lack of clear responsibilities for corporations and host states with respect to human rights, means that very few of the relevant areas of law provide a clear route to state responsibility for the adverse human rights impact of sanctions. Added to this, the two international covenants on human rights were adopted at a time when the importance of modern digital technologies could not have been envisioned, and as legal scholars have pointed out, technological developments tend to outpace the evolution of the law, leaving it outdated and reactive with respect to technological advances.[130]

Although there is currently no legally binding document explicitly addressing the relationship between international human rights law and modern technologies, there has been some development in this area through other sources, including the former UN Special Rapporteur on the promotion and protection of the

[127] Tzevelekos, p. 175; see also Narula, p. 142 (asserting a 'decisive influence' standard based on the ECtHR case of *Ilascu and others v Moldova and Russia*)
[128] Narula, p. 140
[129] Narula, p. 146
[130] Kehl et al, p. 17

right to freedom of opinion and expression, who in a 2011 report stated that 'the Internet has become an indispensable tool for realizing a range of human rights'[131] as well as for 'for full participation in political, cultural, social and economic life.'[132] This statement has formed the basis for further developments regarding human rights in the digital age, culminating in a 2016 HRC resolution passed by consensus which affirmed that 'the same rights people have offline must also be protected online.'[133] Applying this guidance and other rights-specific formulations as to how the content of specific human rights might be interpreted in light of modern technologies, the following chapter will evaluate the human rights impact of technology sanctions as reported in the context of US sanctions in Iran, Syria, and Sudan with regard to both civil and political as well as economic, social and cultural rights. Following from the discussion in chapter 2 covering the extent of the legal obligations owed by the sanctioning state(s) or international organization to individuals in the targeted state, chapter 3 will further endeavor to establish whether such impact may amount to a violation of human rights law incurring state responsibility.

3.1 Civil and Political Rights

Recognized in the aforementioned 2016 HRC resolution on the promotion, protection and enjoyment of human rights on the Internet,[134] modern technologies are particularly important with respect to the right to freedom of expression,[135] the right to privacy,[136] and the right to freedom of peaceful assembly and association.[137] While established as separate articles of ICCPR, these rights are very much interdependent[138] and collectively vital for the exercise of many other human rights.[139] Noted in chapter 1, the importance of ICT tools for the exercise of this set of rights within the context of the Iranian Green

[131] A/HRC/17/27, para 85
[132] A/66/290, para 63
[133] A/HRC/RES/32/13, p. 3
[134] ibid, p. 2
[135] ICCPR Article 19
[136] ICCPR Article 17
[137] ICCPR Article 21 and 22
[138] A/HRC/RES/32/13, p. 2
[139] Robin Elizabeth Herr, "Can human rights law support access to communication technology? A case study under Article 10 of the right to receive information," (Information & Communications Technology Law, 22:1, 2013), p. 1

Movement and Arab Spring was the primary concern of many who suggested that sanctions may have adverse impacts on human rights.[140]

3.1.1 Freedom of Expression

One of the primary rights implicated in technology sanctions, particularly with regards to their impacts on access to the Internet and the tools and resources that it provides, is the right to freedom of expression. The right to freedom of expression and opinion, guaranteed in ICCPR Article 19, is recognized as a uniquely important right to uphold, described by the HRC as 'the foundation stone for every free and democratic society.'[141] Freedom of expression, which can be limited only under certain exceptional circumstances,[142] includes the right to seek, receive, and impart information 'regardless of frontiers' in orally, in writing, in print, or 'through any other media'.[143] The formulation of the right thus introduces an inherent connection between the accessibility of information and the realization of the freedom of expression,[144] and protects both the form and means of expression and dissemination.[145] The CCPR has also highlighted the important role of the press or other media in ensuring the protection of this right[146] and implies that the right includes the protection of a free press which is able to inform public opinion 'without censorship or restraint,' as well as the right of all peoples to receive information from the media.[147] It is also well-recognized that Article 19's accounting for 'any other media' means that the right was drafted with the foresight to accommodate new mediums through which the right might be realized.[148] In the modern era, this expansiveness has typically been applied when considering the right to freedom of expression with respect to the Internet, recognized in both HRC General Comment 34 and even earlier in the 2011 Special Rapporteur report on the right to freedom of expression and opinion as a 'revolutionary' medium unlike any other.[149] However,

[140] see Kehl et al, p. 2
[141] CCPR/C/GC/34, HRC General Comment 34, para 2
[142] ICCPR Article 19(3)
[143] ICCPR, Article 19(2)
[144] Anne Peacock, *Human rights and the digital divide*, (1st edn., London Routledge, 2019), p. 9
[145] GC 34, para 12
[146] ibid, para 13
[147] ibid
[148] UNGA 'Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Frank La Rue' (16 May 2011) UN Doc A/HRC/17/27, para. 21
[149] ibid, para 19

there remains a lack of clarity regarding the scope and content of the right when it comes to the Internet and other ICTs.[150]

In writing on technology sanctions, digital rights advocates and other members of civil society frequently discuss the effects of such restrictive measures on the right to freedom of expression, often arguing that they amount to an impairment of the right.[151] This is typically in the context of reports from Iran, Syria, and Sudan that US sanctions have resulted in severe limitations on the population's ability to access certain tools and resources made available through the Internet, viewed by many as essential to the realization of the right to freedom of expression.[152] They note the heightened importance of these tools within repressive regimes, where the right to freedom of opinion and expression is already limited by the national government through censorship, surveillance, or other means.[153] As activist Dalia Haj-Omar has stated in an appeal to lift US technology sanctions, the Internet is the 'the only platform for free civic engagement in Sudan.'[154]

The former Special Rapporteur on the right to freedom of expression has acknowledged that in contexts where there is very little independent media, ICT platforms 'enable individuals to share critical views and to find objective information.'[155] For example in Iran, where over 60% of the population are Internet users,[156] the government exercises strict control over the media, both online and traditional forms.[157] Likely for this reason, Iran has one of the most active blogospheres in the world,[158] and its 2009 Green Revolution was largely organized over online communications platforms like the end-to-end encrypted Telegram, which at one time had over 40 million active users in Iran.[159] Recognizing this, the government now blocks platforms like Twitter, Facebook, YouTube, and Telegram, in an attempt to expand its control over the information space in the country.[160] This control is facilitated by Iran's development of the National Information Network

[150] Coccoli, p. 228
[151] see Milana Knezevic, "Why US sanctions are a blow to free expression," (Index on Censorship, Jan 31 2014)
[152] Kehl et al, p. 1
[153] Mehta, 791
[154] Jillian York and Kimberly Carlson, "Export regulations on communication and educational technologies loosen for some sanctioned countries and not others—what gives?" (EFF, Feb 27 2014)
[155] A/HRC/17/27, para 19
[156] Tehran Times, "Some 64% of Iranians are internet users: report," (January 11 2019)
[157] Dursun Peksen, "Coercive Diplomacy and Press Freedom: An Empirical Assessment of the Impact of Economic Sanctions on Media Openness," International Political Science Review, (31(4), 2010), p. 453
[158] Ziccardi, p. 240
[159] Center for Human Rights in Iran, "Iran Telegram Ban Strangles Country Amid Struggling Economy, Protests," (June 19 2018)
[160] Mehta, p. 771

(NIN), a state-controlled network which, in addition to numerous security issues and content restrictions, separates domestic internet traffic from international, enabling the government to sever access to the global internet at will.[161]

Given the control that states may exercise over the media, access to independent sources of information available on the global internet and social media platforms are vital for people to share and receive information freely. Tech savvy users in Iran have been able to access these platforms through virtual private networks (VPNs) or products like the popular Toronto-based Psiphon (not subject to US sanctions) which enable users to circumvent government filters and censors, as well as conceal their online activity.[162] However, VPNs are increasingly difficult to access in states which are subject to US sanctions. As a result of the sanctions, US-based companies like Amazon and Google have blocked access for Iranians to some of their products, notably Amazon Web Service (AWS), the Apple App Store, as well as the Google Play Store and Google App Engine (GAE).[163] AWS is one of the world's most extensive cloud computing platforms and was reportedly used by Iranian developers to create open-source VPNs for public consumption.[164] Amazon's sanctions-related blocking of this product will force developers of all tools, not just VPNs, to use state digital services provided by the NIN, which will only strengthen the government's ability to control Iranians' access to the internet and reduce the possibility for circumvention.[165] Similar to a VPN is another popular circumvention tool, Tor, which is widely used across the globe by Internet users seeking to evade government censorship and surveillance, using a technique called "domain fronting" to conceal network traffic from surveillance and bypass government censors.[166] Unfortunately, domain fronting relies on the GAE, which is no longer available in Iran and thus leaves Tor as yet another unavailable tool for gaining access to diverse sources of information and maintaining some form of free and open media.[167]

---

[161] Center for Human Rights in Iran, "Guards at the Gate: The Expanding State Control Over the Internet in Iran," (2018), p. 26

[162] see note 7

[163] Mahsa Alimardani and Roya Pakzad, "Silicon Valley preaches diversity and inclusion while excluding Iranians," (Atlantic Council, 2019)

[164] Center for Human Rights in Iran, "More Iranians Forced to Rely on Unsafe Online Hosting After Amazon Ban," (August 7, 2019)

[165] ibid

[166] Lorenzo Franceschi-Bicchierai and Jason Koebler, "Microsoft and Amazon Enable Censorship Circumvention Tools in Iran. Why Doesn't Google?" (Vice, Jan 15 2018)

[167] Alexander Martin, "Google faces calls to lift anti-censorship blocks in Iran," (Sky News, January 2, 2018)

The impacts of sanctions-related restrictions on US technology products and services extends far beyond VPNs. Iranian individuals and companies commonly use cloud computing platforms like AWS and GAE to host their websites and online services as opposed to the NIN, meaning that much of the independent Internet will now be forced onto the heavily censored government-run network.[168] As a further consequence, other international websites that are hosted on AWS may no longer be available in the country, reducing the available online resources for the Iranian population.[169] Additionally, prior to the issuing of General Licenses by the US revising sanctions regimes in Syrian, Sudan and Iran, the effects of the sanctions were much farther reaching, prohibiting the sale of both software and hardware, including antivirus software, secure chat applications, laptops, and cell phones.[170] Thus, in each of these cases and to varying degrees, the impact of sanctions on the accessibility of the Internet as means of both receiving and disseminating information has been reported, and some argue that limiting the Internet in this way, and depriving individuals of the tools they need to access it, interferes with the right to freedom of expression.[171] In order to evaluate this assertion, this section will consider whether access to the Internet is protected under the right to freedom of opinion and expression, what the scope and content of the obligations might be with respect to the Internet, and whether the reported effects of technology sanctions amount to a breach of those obligations given the models of extraterritorial jurisdiction discussed in chapter 2.

The clearest starting point for this analysis is HRC General Comment 34, which following from Article 19's inclusion of the phrase 'any other media' in reference to the protected means of expression, asserts that this includes all forms of audio-visual as well as electronic and internet-based modes of expression.'[172] It further states that parties to the ICCPR should 'take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto,'[173] suggesting that state parties carry certain obligations with respect to the people's ability to access these technologies given their importance as a means of realizing the right to freedom of opinion and expression. While some have extended this argument

[168] see note 164
[169] ibid
[170] Danielle Kehl, "US Government Clarifies Tech Authorizations under Iranian Sanctions," (New America, Feb 12, 2014)
[171] Mehta, p. 812
[172] GC 34, para 12
[173] ibid, para 15

to advance the notion of an independent right to the Internet,[174] it would seem that given the lack of consensus around such a claim and the content of the proposed right, proceeding on the basis that the Internet is an important and protected means of realizing the right to freedom of expression is the correct approach.

Freedom of expression, like many other civil and political rights, is conceived of in primarily negative terms, establishing acts or omissions of the state which might amount to a violation of the right. General Comment 34 accordingly establishes a negative obligation with respect to Internet access, such that '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,' must be compatible with the clause on acceptable limitations.[175] Further, 'permissible restrictions generally should be content-specific,' rather than generic.[176] This has been elaborated on in the ECtHR case, *Yildirim v Turkey*, in which the Court ruled that the government's blocking of all Turkish-based Internet users from the hosting platform Google Sites in order to remove one site facing criminal proceedings, was unjustified and a violation Article 10 on freedom of expression.[177] While the Court acknowledged that restrictions on access to certain contents of the Internet may be permissible, it recognized that Google Sites constitutes a means of exercising the right to freedom of expression 'in light of present day conditions' and found that the effects of the government blocking of Google Sites in its entirety produced arbitrary effects.[178] It also asserted that, as the Internet is now a 'principle means' by which people exercise the right to freedom of expression, any blocking measure is bound to influence the accessibility of the Internet and engage State responsibility under Article 10.[179] Later cases of *Kalda v. Estonia*[180] and *Jankovski v. Lithuania*,[181] lend further support to this decision, asserting that given the unique

[174] Coccoli, p. 243
[175] GC 34, para 43
[176] ibid
[177] *Yildirim v. Turkey*, App no 3111/10 (ECtHR, 18 December 2012), para 69
[178] ibid, para 67
[179] ibid, para 54
[180] Kalda v. Estonia, Application no. 17429/10 of 19 January 2016, para 50
[181] Jankovski v. Lithuania, Application no. 21575/08 of 17 January 2017, para 40

nature of online content and means of dissemination, there may be no 'alternative means' with the same capabilities available to individuals affected by a blocking measure.[182]

Certainly, an argument could be made that blocking access to multiple cloud computing platforms and communications platforms, as US sanctions have reportedly done in Iran, Syria and Sudan, is similar to that of blocking access to Google Sites as considered in *Yildirim v Turkey*, and if carried out within US territory, may similarly amount to a breach of state obligations. Both Google Sites and the tools restricted under US sanctions influence the accessibility of the Internet and thus may be protected from arbitrary interference under ECHR Article 10, and probably by extension ICCPR Article 19. However, while the above considers the obligations of the territorial state to refrain from arbitrarily blocking substantial parts of the Internet for its citizens, in the context of technology sanctions what must be addressed is whether the sanctioning state, in imposing restrictions on access to products which could allow for and contribute to a freer and more open Internet in Iran, may violate its obligations with respect to the right to freedom of opinion and expression extraterritorially.

As discussed in chapter 2.1.1, under the emerging recognition of extraterritorial jurisdiction on the basis of one state exercising power or control over the enjoyment of particular civil and political rights in a foreign state (the 'impact model'),[183] as well as the 'causation model' asserted by the IACtHR,[184] it is conceivable that a state imposing sanctions on technology which impact access to the Internet as a means of exercising the right to freedom of expression might breach its extraterritorial obligations under Article 19. Certainly, if the sanctioning state were in control of the Internet service providers in the targeted state and prohibited their operation, or itself effected the blocking of massive online platforms like Facebook, Telegram, or Twitter, a strong case could be made that that state exercised 'power or control' over the right to freedom of expression and opinion, as is required under the impact model. Likewise, under the causation model, it could be said that the US exercised effective control over a policy which directly caused serious and foreseeable harms that negatively impacted the right to freedom of expression. Given the relative importance of these particular products and services for accessing the Internet and receiving and

[182] see also *Appleby v. United Kingdom* ECHR 2003-VI
[183] see GC 36, para 63
[184] see chapter 2.1.3

disseminating information online, enforcing a measure which restricted access to them would likely satisfy either of these more flexible bases of jurisdiction. As such, a much stronger argument could be made for a violation of US extraterritorial obligations with respect to earlier sanctions regimes prior to the issuing of general licenses, which reportedly had much more far-reaching effects, targeting the majority of hardware and software with US components.[185]

In the abovementioned cases of policies which amount to the blocking of certain platforms used in the development of VPNs, it seems less likely that this would not meet the threshold of control over the right required to assert extraterritorial obligations under the impact model,[186] nor the undefined 'seriousness' threshold of the causation model. While important tools for circumventing censors, particularly in places where governments exercise significant control over the means of disseminating and accessing information, control over the availability of certain VPNs and other tools linked to particular cloud computing platforms would likely not amount to power or control over access to the Internet as a means of realizing the right to freedom of expression. The impact would also not be direct, as sanctions are not themselves blocking access to the Internet, but rather heightening the effects of Iranian filters and censors by limiting options for bypassing them and accessing the global Internet. As evidenced by the existence of tools like Psiphon and other national alternatives,[187] although some of these may be less secure, it would appear that there are suitable 'alternative means' of accessing the Internet which render VPNs and other products and services originating from the sanctioning state non-essential for the realization of the right.

While the above analysis focuses on a state's obligation not to interfere with access to the Internet, according to a joint declaration published by the UN Organization for Security and Co-operation in Europe (OSCE) states may also have positive obligations under the right to freedom of expression 'to *facilitate* universal access to the Internet.'[188] Although this declaration is not legally binding, it still carries the support of experts in this rights area from each of the major regional human rights systems and has been restated,

[185] see note 170
[186] GC 36, para 63
[187] see note 7
[188] UN OSCE 'Joint Declaration on Freedom of Expression and the Internet' (1 June 2011), para 6(e)

albeit to a lesser extent, in other UN resolutions[189] and General Comment 34.[190] However, such an obligation, according to Martinovic, would be subject to the degree of effective control exercised in the targeted state.[191] Sanctioning states, not often exercising effective control in the targeted state, would thus rarely incur such positive obligations. That being said, the HRC has encouraged States to 'take steps to prevent abuse abroad by business enterprises within their jurisdiction.'[192] While companies like Google, Amazon, and Apple have justified their actions in limiting certain technologies on compliance with US sanctions, as some have argued, platforms such as AWS and GAE likely are not prohibited under the current sanctions regimes, yet the companies have still elected to block them in targeted states.[193] Part of this may be due to the lack of policy clarity provided by the sanctioning state as to what should be restricted under the current sanctions regimes and a failure of the state to take positive action to ensure that non-state actors do not infringe on the rights of the targeted state's population. As discussed in chapter 2.2, if the above were true, a case could be made for the indirect attribution of extraterritorial human rights violations if the sanctioning state failed to satisfy its due diligence obligations.[194] This would have to be evaluated in light of whether individual private actors could be directly linked to an infringement of human rights in the target state, and whether the sanctioning state took all reasonable measures to protect against the infringement given the circumstances of the particular situation.[195] Factors such as the number of general licenses passed to clarify and loosen sanctions restrictions, communications and responsiveness to the concerns of the private sector regarding sanctions compliance, the reliability and availability of impact reports, and engagement with relevant stakeholders might all be considered in determining state responsibility.[196]

[189] see UN Doc A/HRC/20/L.13; States should 'promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries'
[190] State parties should 'take all necessary steps to foster the independence of these new media and to ensure access of individuals thereto'; see GC 34, para 15
[191] Milanovic, p. 209
[192] UNGPs, Principle 3
[193] see note 164
[194] see note 126
[195] Cedric Ryngaert, 'Jurisdiction: Towards a Reasonableness Test,' in Langford et al (eds), p. 204; see also *Velasquez Rodriguez v Honduras*, para 172
[196] Narula, p. 146

Finally, considering that private companies within the ICT industry have been referred to as 'indispensable to the contemporary exercise of freedom of expression,'[197] and the fact that their actions can have significant impact on the exercise of the right, private actors may also have responsibilities with respect to the effects of technology sanctions.[198] Companies should thus ensure that in complying with technology sanctions, they carry out effective due diligence in order to identify, prevent and mitigate potentially adverse impacts on the right to freedom of expression.[199] While in some cases, their ability to do this depends on improvements or revisions of sanctions policies, in certain circumstances, technology companies have clearly practiced overcompliance to the detriment of human rights. For instance, in December 2018, the platform Slack banned all users of its product who had ever connected to the platform from an Iranian IP address, despite the fact that these individuals may be fully entitled to use the platform under the US sanctions regime.[200] If true, this sweeping response to sanctions certainly would likely have the effect restricting access to users who were legally entitled to use its services and would amount to a failure of that company to uphold its responsibility to respect human rights.

3.1.2 Right to Privacy

Sanctions have also had the effect of severely hampering the ability of target populations to communicate securely and privately, a necessary component of the right to freedom of expression and opinion and a fundamental principle of the right to privacy, protected under ICCPR Article 17. The right to privacy includes the freedom from arbitrary interference by state authorities or private actors with one's family life, personal relationships, and most relevant in this context, correspondence.[201] It is considered an enabling right, in that is an important condition for the exercise of other Convention rights such as freedom of expression and opinion as well as freedom of assembly and association.[202] States carry both a negative obligation to refrain from such arbitrary or unlawful attacks on privacy as well as a positive obligation to

[197] A/HRC/35/22, para 47
[198] see chapter 2.2
[199] UNGPs, Principle 17
[200] "Joint submission to the Universal Periodic Review of the Islamic Republic of Iran by ARTICLE 19 and Access Now," (April 4, 2019), para 45
[201] ICCPR Article 17(1)
[202] see UNGA Res. 68/167; see also A/HRC/13/37 and A/HRC/RES/20/8

adopt 'legislative or other measures to give effect to the prohibition' of such interferences.[203] In order for the right to privacy to be upheld, 'the integrity and confidentiality of correspondence should be guaranteed,' and 'correspondence should be delivered to the addressee without interception and without being opened or otherwise read.'[204] Thus, the right serves to limit a state's ability to monitor and surveil its citizens and protects a 'zone of privacy' which enables the enjoyment of other rights and an individual's ability to participate freely in political, economic, social, and cultural life.[205] The restriction of arbitrariness thus establishes that any interference with the right must established by law, necessary to achieve a legitimate aim, and proportional.[206]

In the case studies examined, the impact of US sanctions on the right to privacy primarily concerns restrictions on access to encrypted communications software and other personal security tools, which enable individuals to protect themselves against unlawful surveillance. Encryption refers to the scrambling of data so that only intended recipients are able to access it and is one of the most popular tools for protecting the security of individuals and their communications online.[207] Prior to its blocking by the government in 2018, Iranians had primarily relied on the tool Telegram to send end-to-end encrypted messages to bypass government surveillance and communicate freely.[208] As an alternative, Iranians could turn to Signal, a more secure application used globally to evade surveillance and maintain private communications.[209] However, Signal relies on 'domain fronting' and uses the Google App Engine which is restricted for Iranian Internet users.[210] While not having access to Signal might not be seen as a significant absence in Iranian society, combined with the regimes successful blocking of Telegram and WhatsApp,[211] the two most common encrypted communications tools, Iranians are left with few options for protecting their privacy while sending messages online. Sanctions have also reportedly interfered with security features such as two-factor authentication (2FA), which adds an additional layer of verification to prevent

[203] CCPR General Comment 16, para 1
[204] ibid, para 8
[205] A/HRC/29/32, para 15
[206] GC 16, para 4
[207] A/HRC/29/32, para 1
[208] see note 159
[209] see note 7
[210] ibid
[211] see A/HRC/29/32, para 39

unauthorized logins of user accounts. For instance, Google bars the distribution and promotion of its Titan key for 2FA in countries under US sanctions and users have also reported being unable to access Twitter's 2FA system which uses SMS messages sent to cellphone number.[212]

A common feature of technology sanctions is that they often force individuals within targeted countries to rely on alternatives which are less protective of human rights and make them more vulnerable to surveillance and censorship.[213] Thus, when US technology and security updates are not available, it facilitates repression from authoritarian regimes and makes it easier for them to compromise the security and privacy of vulnerable individuals. For instance, seeking circumvention tools to bypass government censors, individuals in Syria turned to a proxy software called Simurgh, which could easily be attained and shared on portable discs.[214] However, given the unofficial nature of this product and insecure distribution, some versions of this tool were being circulated with a malicious 'backdoor' which would allow third parties to access user information and activity.[215] Throughout the anti-government protests of the Arab Spring, Syrian activists were reportedly subject to many such malware attacks because they also could not access the Google Play Store or Apple App Store to download legitimate versions of apps, instead turning to unknown or unofficial sources of these products.[216] The sophisticated nature of the Syrian regime's cyber operations allowed government actors to exploit this unofficial app market, which arose as a consequence of sanctions, to seed malicious software and target activists and dissidents.

This increased susceptibility to surveillance for individuals in states targeted by technology sanctions, often combined with the heightened surveillance and censorship efforts of the targeted state on its population, can have dire consequences. In Iran, online targeting of journalists, human rights activists, and other members of civil society is widespread.[217] Arrests and severe sentences are common for the country's active bloggers and online critics, some even receiving death sentences for their online posts, convicted of

[212] Joseph Cox, "Google Gives Free Security Keys to Activists, But Not if You're in Iran or Syria," (Vice, April 26, 2019)
[213] Kehl et al., p. 2
[214] Morgan Marquis-Boire, "Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor," (May 25, 2012)
[215] ibid
[216] Danielle Kehl and Tim Maurer, "Confusing Sanctions Are Aiding Government Repression," (Slate, May 30 2013)
[217] see A/HRC/29/32, para 34

charges such as “insulting the Supreme Leader” and “propaganda against the regime.”[218] Lacking access to encryption tools and other forms of secure communication, and forced to use more vulnerable tools in lieu of international tools restricted under US sanctions, this lack of privacy has a chilling effect on society and democratic participation.[219] As a result, many individuals including journalists and human rights defenders refrain from organizing or expressing themselves out of fear of being targeted by the regime for their views and acts.[220] Thus, repeated interferences with right to privacy, as in the case of targeted state surveillance, has effects not only on the individuals whose correspondences are intercepted, but also on society as a whole and their right to freedom of expression.[221]

It is clear that in many of the states subject to US sanctions, the right to privacy is increasingly under threat, as are other rights which privacy enables such as the right to freedom of expression and opinion.[222] Given that in a number of reported cases in the countries examined, correspondences are intercepted and analyzed by the state without legitimate reason and without proper regulation or oversight,[223] it would appear that in many instances, interferences with the right would be held to be arbitrary or unlawful under international human rights law.[224] Recognized in the jurisprudence of the ECtHR, the protections against arbitrary interference with correspondence under the right to privacy extends to digital correspondence,[225] and HRC General Comment 16 even goes so far as to assert that *all* surveillance of conversations, including electronic, ‘should be prohibited.’[226] While this statement seems to ignore that the right specifically prohibits *arbitrary or unlawful* interference, as well as jurisprudence holding surveillance to be lawful in certain cases,[227] it reinforces that surveillance of digital correspondence is fundamentally at odds with the right to privacy and must be strictly limited.

In accordance with this, the 2017 HRC report titled ‘The Right to Privacy in the Digital Age’ asserts an important role for the security of technologies and, in particular, the availability of encryption for the

[218] ibid
[219] A/HRC/32/38, para 57
[220] A/HRC/38/35/Add.2, para. 53
[221] A/HRC/41/35, para 21
[222] A/HRC/29/32; and A/HRC/23/40, para. 24
[223] “Guards at the Gate”, p. 36
[224] see *Liberty and Others v. the United Kingdom*, ECtHR Application no. 58243/00, 1 July 2008, para 69
[225] ibid, para 56
[226] GC 16, para 8
[227] see *Klass and Others v.* Germany, ECtHR, Application no. 5029/71, 6 September 1978

protection of the user against such unlawful interference.[228] Furthermore, the broad concept of 'correspondence' in Article 17 would seem to allow for new manifestations of the scope of protection of the right to privacy. Thus, in the era of electronic and networked communications through email, peer-to-peer messaging applications, and platforms like Twitter, the right to privacy should encompass protections against interferences with these forms of correspondence through encryption or other tools.[229] Noting the interdependence between the right to privacy and the right to freedom of expression, the two most recent Special Rapporteurs on the latter right have asserted the importance of encryption technology specifically, as it can act as a 'zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks.'[230] Following from this argument, a 2016 UNESCO report titled 'Human Rights and Encryption' links encryption to the protection of 'uninhibited communications,' [231] which have been recognized by the ECHR as a precondition for freedom of communication.[232] The report bases its argument for the legal protection of encryption on the notion that encryption is a second level right and a required precondition for the right to privacy and freedom of expression to be realized.[233] Thus, it argues that 'restriction of the availability and effectiveness of encryption as such constitutes an interference with the freedom of expression and the right to privacy…Therefore, it has to be assessed in terms of legality, necessity and purpose.'[234]

As illustrated, there is strong support for considering access to encryption and the necessary tools for anonymity as a fundamental component of the right to privacy in the digital age, as well as the right to freedom of expression and opinion. However, the extent of state obligations with respect to these technologies seems dependent on the particular conception of encryption under the right to privacy. For instance, the UNESCO report argues that encryption is not just a *means* of protecting the right to privacy online, but a necessary precondition for the right to be protected in digital spaces.[235] Thus, states may have a negative obligation to refrain from imposing any restrictions on the accessibility of encryption as this would

[228] A/HRC/RES/34/7
[229] Wolfgang Schulz and Joris van Hoboken, "Human rights and encryption," (UNESCO 2016), p. 52
[230] see A/HRC/29/32, para 16 and A/HRC/23/40, para 89
[231] Schulz and Hoboken, p. 54
[232] see *Cumhuryiet Vafki and others v. Turkey*, ECHR 10.08.2013; *Ricci v. Italy*, ECHR 10.08.2013 - 30210/06.
[233] Schulz and Hoboken, p. 55
[234] ibid; see also A/HRC/29/32, para 56 and A/HRC/RES/34/7, para 9
[235] Schulz and Hoboken, p. 55

amount to an interference with the right to privacy. Alternatively, under a more straight-forward reading of ICCPR Article 17, given that the right only explicitly prohibits 'arbitrary or unlawful interference' with an individual's privacy, the sanctioning state might only be said to indirectly contribute to a violation of the right to privacy in the target state by restricting access to the tools individuals need to protect their privacy and security. Thus, providing access to encryption and security tools may only amount to a positive obligation to ensure the right to privacy by enabling individuals to protect themselves against unlawful interferences by other actors.[236]

Under both interpretations, as in the above section, the argument of whether the sanctioning state may have committed a violation of its obligations rests on whether or not it exercises extraterritorial jurisdiction in the targeted state. If one takes the approach advocated by UNESCO, that any interference caused by sanctions on the accessibility or effectiveness of encryption amounts to a breach of a state's negative obligations to respect the right to privacy,[237] a violation seems plausible under either the impact or causation models. Subject to a determination of seriousness of the impact or harm and the foreseeability of this impact, sanctions-related restrictions on encryption tools would likely amount to a direct interference with the right to privacy under this interpretation of the right. As in the previous section, under the impact and causation models, the existence of substantial impact amounting to power or control over the right to privacy would also need to be considered in terms of the availability of an alternative means for encryption as well as the due diligence exercised by the state imposing such sanctions.[238] Alternatively, if protecting access to encryption is a positive obligation of state parties to the ICCPR, it could be said that denying access to such tools in the targeted state, as US sanctions have been shown to do, also amounts to a violation of a state's positive obligations to secure and ensure the right to privacy.[239] However, as noted previously, even those who advocate for a broader understanding of extraterritorial jurisdiction have suggested that such obligations are limited to situations where the state exercises effective control.[240]

[236] GC 16, para 1
[237] see note 235
[238] see *Kalda v Estonia* and *Jankovski v. Lithuania*
[239] GC 31, para 8
[240] Milanovic, p. 210

Private actors are also implicated in the effects of sanctions on the right of privacy, as it often their decision to refuse to update or suspend the provision of services or products to targeted states. In some cases, it may not be entirely clear whether a certain product is restricted under a particular sanctions regime, as seems to be the case with the Google Titan key, which was restricted based on internal decisions at Google to bar distribution of these products in countries under US sanctions.[241] As discussed in chapter 2.2, if this lack of policy clarity leads to an interference with the right to privacy and is the result of negligence on the part of the sanctioning state with respect to its due diligence obligation, this might provide grounds for the indirect attribution of an extraterritorial human rights violation to the state.[242] Additionally, under their responsibility to respect human rights throughout their global operations, companies should endeavor to provide vital privacy and encryption tools where possible,[243] as well as collect feedback from affected stakeholders as to the effects of sanctions and the absence of certain products and services on their rights.[244] Under the responsibility to carry out due diligence, corporations should also engage in discussions internally about how to respond to sanctions policies, its implications for the security of their products, and the appropriate way to respond to minimize or negate such impacts.[245]

3.1.3 Freedom of Assembly and Association

Given its interrelated and interdependent nature with the rights discussed in the previous two sections, the right to freedom of assembly and association, protected under ICCPR Articles 21 and 22, is also implicated in the impact of technology sanctions. Together, the rights protect the freedom of individuals to associate with others and engage in peaceful assembly, subject only to limitations prescribed by law and necessary in a democratic society.[246] The right of peaceful assembly is recognized by the HRC as the 'foundation of a system of government based on democracy, human rights and pluralism'[247] and imposes

[241] see A/HRC/32/38, para 57
[242] see note 124
[243] A/HRC/29/32, para 28
[244] UNGPs, Principle 20
[245] UNGPs, Principle 17
[246] ICCPR Article 22 (1)
[247] HRC 'Draft General Comment 37', para 1

an obligation on state parties to accommodate, and indeed facilitate, such assemblies.[248] As the UN has noted, both the right to privacy[249] as well as the freedom of expression[250] are integral to the enjoyment of the right to freedom of association and assembly. If individuals do not have the tools to communicate and share information or if they feel their privacy is threatened by surveillance or other forms of monitoring, they are unlikely to be able to exercise freely their right to association or assembly. The exercise of the right has also been linked with modern technologies, which have fundamentally changed the ways public assemblies are organized and carried out, presenting both risks and possibilities.[251] For example, certain social media platforms may be tremendously useful for coordinating assemblies, while online surveillance may expose greater numbers of people to targeting and persecution for their participation.[252]

As such, many of the sanctions-related effects discussed in Chapter 3.1.1 and 3.1.2 would likely have serious implications for the right to freedom of assembly and association. For one, the ability to freely share and access information as protected under the right to freedom of expression is also vital for individuals to organize peaceful assemblies.[253] Thus, limitations on secure communication tools and VPNs, which enable individuals in repressive regimes to access social media like Facebook and Twitter as well as other digital sources of information, would have an impact on the right to freedom of assembly as well. Certainly, there are other means of disseminating information about an assembly, however, particularly, where the state exercises substantial control over communications infrastructure, it is unlikely that organizing through phone calls or text messages will be a secure mode of bringing individuals together, not to mention the inefficiency of this method compared to other mass communications tools like Facebook or Telegram.[254] Telegram for example allows for secure group messaging between thousands of individuals at once, enabling the organization of large-scale assemblies while protecting against unlawful breaches of the right to privacy.[255] As for other alternatives, while use of social media like “Hotgram” and “Telegram Talaee” in Iran might technically provide the tools to facilitate assemblies, the fact that such products are tied to the

[248] ibid, para 7
[249] A/HRC/RES/34/7
[250] GC 34, para 4
[251] Draft GC 37, para 12
[252] A/HRC/41/41, para 2
[253] A/HRC/23/39, para 72
[254] Ziccardi, p. 194
[255] see note 159

NIN compromises the security of gathering organized on those platforms and enhances the ability of the Iranian regime to suppress the opposition's ability to mobilize against it.[256] Further, when sanctions deprive individuals of security and encryption tools, it not only impacts their digital privacy, but heightens the risk to themselves and other of being targeted for their association with a protest or activist network. The digital domain is now a primary battlefield for governments targeting members of civil society, as they may be able to gain access to an individual's contacts and target their associates, suppress movement organizers, and conduct surveillance operations at mass gatherings.[257] This may lead to both direct interferences with rights, including the right to freedom of assembly and association, as well as a chilling effect on the exercise of this right across society as whole.

Still in its draft stage, General Comment 37 on the right to peaceful assembly notes that considerations of the role that technology plays in exercising the right must 'inform an assessment of the legal framework required to give full effect to article 21 today,'[258] suggesting that future interpretations as to the content of the right to peaceful assembly will more specifically address the role of technology. In 2019, the Special Rapporteur on the rights to freedom of peaceful assembly and of association suggested the essential nature of online platforms like Facebook and Twitter for the right to peaceful assembly, referring to them as 'gatekeepers to people's ability to enjoy the rights of peaceful assembly and association…and participate in the democratic space.'[259] The Special Rapporteur also appears to argue for the role of digital technology, not just as means of facilitating assembly and association in person, but also as a virtual space where the right can be exercised.[260] Thus, while assembly has generally been understood as a physical gathering of people, human rights protections 'may apply to analogous interactions taking place online.'[261] As such, free and open access to virtual spaces could be asserted as a necessary protection under the right to peaceful assembly in addition to the traditional understanding of the right as pertaining to assemblies in physical public spaces. In light of this, the Special Rapporteur has called on states to '*ensure* that everyone can access and use the Internet to exercise these rights and that online associations and assemblies are

[256] "Guards at the Gate," p. 26
[257] A/HRC/41/41, para 65
[258] GC 37, para 12
[259] A/HRC/41/41, para 4
[260] ibid, para 11
[261] A/HRC/38/L.16, Preamble

facilitated in accordance with international human rights standards.'[262] Taken together, the above statements seem to assert a positive obligation on state parties to ensure and facilitate assemblies online by providing access to an open and free Internet.

It is thus clear that the Internet and other digital tools are widely recognized as integral to the exercise of the right to freedom of assembly as well as standalone spaces in which assemblies can take place. Following the analysis of 'alternative means' in chapter 3.1.1, it would likely be the case that other means of organizing and assembling would not be considered suitable alternatives given the unique capabilities of the Internet to provide an efficient and cost effective form of mass communication, as well as a separate digital space for vulnerable groups to assemble free of public persecution. Furthermore, based on the above analysis, it appears that states may have both a negative obligation not to *interfere* with access to these digital tools as well as a positive obligation to *facilitate* access to these tools for individuals within their territory or under their jurisdiction.

As to the question of extraterritorial jurisdiction in the context of technology sanctions, roughly the same arguments established above in relation to circumvention and encryption tools would apply here as well. Considering that what would likely be protected under the right to freedom of association and assembly is access to a free and open Internet as a space for both organizing and participating in peaceful assemblies, the reported effects of US technology sanctions as discussed in chapter 3.1.1 and 3.1.2 would likely not satisfy the threshold of 'power or control' over access to the Internet, nor would the impact be 'serious' enough to constitute an extraterritorial violation under either the causation or impact model of jurisdiction. However, given that social platforms like Facebook, Twitter, and Telegram might be recognized as equivalent to physical spaces of assembly,[263] if technology sanctions were to affect a complete shutdown of one or all of these platforms for which few alternatives exist, an argument could be made that the sanctioning state does in fact exercise 'power or control' over freedom of assembly *online* or exercises effective control over the act which directly causes the interference with the right. While such effects have not been reported in any of the case studies examined or otherwise, if sanctions had this impact, it would

[262] A/HRC/41/41, para 11
[263] ibid

likely amount to a breach of the sanctioning state's extraterritorial obligations not to interfere with the right to freedom of assembly and association.

The current Special Rapporteur on the rights to freedom of peaceful assembly and of association has also noted that digital technology companies have played a significant role in creating challenges for individuals and organizations seeking to exercise these rights online as well as offline.[264] As such, he asserts that these companies 'must commit to respect freedoms of peaceful assembly and association and carry out due diligence to ensure that they do not cause, contribute to or become complicit in a violation of these rights.'[265] Thus, while companies would not be held legally liable for refusing to provide certain services to targeted states on the basis of sanctions, they should adhere to the Principle 17 of the UNGPs in identifying risks to stakeholders and their rights to peaceful assembly and association, and communicate with their home government about such risks and impacts. As discussed in chapter 3.1.1, if companies such as Facebook or Twitter were under a state's jurisdiction and decided to restrict access to their services in response to sanctions (which as mentioned might amount to a breach of the right to freedom of assembly and association), this infringement might be indirectly attributable to the state subject to an assessment of its exercise of due diligence to respond to and remedy the illicit conduct of the non-state actor.

3.2 Economic, Social, and Cultural Rights

In addition to their importance for the exercise of civil and political rights in the digital age, the Internet and other ICTs are also recognized as an enabler of the economic, social, and cultural rights enumerated in the ICESCR.[266] Such technologies increasingly play a dominant role in every aspect of life in modern human societies, serving as intermediaries and access points for growing number of ICESCR rights, including the right to education (Article 13), the right to take part in cultural life and enjoy the benefits of scientific progress and its applications (Article 15), the right to work (Article 6), the right to health (Article 12) and others.[267] Thus, the impacts of technology sanctions on ESC rights also merits consideration in the context of this analysis. In fact, given the international framing of the scope of rights obligations under the

[264] A/HRC/41/41, para 65
[265] ibid, para 67
[266] A/HRC/RES/34/7; A/68/362, para 3
[267] Peacock, p. 21

ICESCR and the absence of a jurisdictional clause,[268] it could be argued that the ICESCR provides a more suitable legal framework for addressing the adverse impacts of technology sanctions.

3.2.1 Right to Education

The right to education, protected under articles 13 and 14 of ICESCR, first defines that education 'shall be directed to the full development of the human personality and the sense of its dignity,' and 'enable all persons to participate effectively in a free society.'[269] In General Comment 13, CESCR acknowledges the importance of the right to education as an empowerment right, serving as 'the primary vehicle by which economically and socially marginalized adults and children can lift themselves out of poverty and obtain the means to participate fully in their communities.'[270] CESCR further describes the essential features of education that states are obligated to provide for, which are *availability, accessibility, acceptability, and adaptability*.[271] Notably, physical accessibility includes education via modern technology such as "distance learning" programs.[272] Finally, outside of a state party's jurisdiction, General Comment 13 asserts that states are under an obligation to 'provide international assistance and cooperation for the full realization of the right to education,' including to ensure that their actions as part of international organization 'take due account of the right to education.'[273]

In the digital age, ICTs play an increasingly important role with respect to this right, enabling access to educational materials and other modes of online learning which are 'revolutionizing the provision of education.'[274] Massive open online courses (MOOCs) may provide an 'alternative path to higher education' and open educational resources can provide access to materials, knowledge, and information where it would otherwise be unavailable.[275] Given this transformed education landscape, it should not come as a surprise that Special Rapporteur Idriss Jazairy, after his country visit to Sudan in 2016, reported that

[268] see chapter 2.1.2
[269] ICESCR Article 13(1)
[270] CESCR General Comment 13, para 1
[271] ibid, para 6
[272] ibid, 6(b)
[273] ibid, para 56
[274] A/HRC/32/37, para 27
[275] ibid, para 30

sanctions enacted by the US which target technological resources 'also affect the right to education.'[276] He included in his report that citizens of Sudan are 'deprived of scholarship opportunities and of software and other technology, which would allow them to improve and update resources for teaching and learning,'[277] and to participate in trainings and exchanges via the Internet.[278] For instance, in 2014, a graduate student studying software engineering reported having her graduation project severely interfered with as a result of US sanctions, which left her unable to access various software components of the mobile app she had been developing as well as educational materials and guides on how to use certain integral technologies.[279] A number of MOOCs and educational platforms like Coursera, which provides access to online courses and credentials, are also restricted to users in Sudan, Iran,[280] and until recently, Syria.[281] In Sudan, demand for these technologies is reportedly very high, with one activist claiming that many are turning to MOOCs and online educational resources as 'many youth realize that they can't compete regionally or nationally if they don't have better education.'[282] Universities have also been reported using these resources to supplement curriculums due to the difficulty and high cost of accessing hard copy educational materials.[283]

While individuals whose access to online educational resources has been impacted by sanctions clearly identify it as a significant barrier to education, as does the Special Rapporteur on the negative impact of unilateral coercive measures, it is unclear whether access to such resources is protected by international human rights law. Certainly, the value of MOOCs and other ICTs for realizing the right to education is recognized by CESCR[284] as well as the current Special Rapporteur on the Right to Education.[285] However, the Special Rapporteur also highlights the negative impacts that digital technologies can have on the right to education, notably their role in expanding the digital divide when only certain schools can provide

[276] A/HRC/33/48/Add.1, para 25
[277] ibid
[278] ibid, para 46
[279] Amanda Sperber, "In Sudan, Civil Society says It's Struggling to Work Around US Sanctions' Block on Tech," (TechPresident, January 14 2014)
[280] A similar educational resource, Khan Academy, also restricts access to Iranians; Jillian York and Kimberly Carlson, "Sudan Tech Sanctions Harm Innovation and Development: US Government and Corporations Must Act," (EFF, June 26, 2014)
[281] see Kehl 2014
[282] see note 280
[283] ibid
[284] GC 13, para 6
[285] A/HRC/32/37, para 37

technological tools, and the practice of some states to outsource the provision of education to private entities.[286] Thus, it could hardly be said that there are legal grounds for claiming that state parties are obligated to provide such technologies as part of the right to education, although such tools may assist in meeting existing obligations. Further, while the availability and accessibility of education is an obligation of states and may include in part access to digital teaching materials and online education restricted under sanctions,[287] these obligations specifically apply with respect to individuals under a State's jurisdiction and thus most likely wouldn't be relevant in this context.[288]

That being said, particularly given the reported lack of access to certain educational materials and services in countries like Sudan and Syria, which has resulted in the heightened importance of digital resources, sanctioning states may see the provision of such tools as a part of their obligation to take steps 'through international assistance and cooperation, especially economic and technical,' towards the full realization of the right to education.[289] However, as noted in chapter 2.1.2, the nature of this obligation is not well understood and many Western states consider it only a moral obligation.[290] The predominant view of legal scholars who recognize this obligation seems to differentiate the degree of state responsibility to ensure ESC rights extraterritorially on the degree of control exercised.[291] Again, as sanctioning states rarely exercise substantial control within the target state, and as digital education resources should only be considered supplementary to the educational system within the targeted state, it is likely that the sanctioning state would only have a negative extraterritorial obligation not to interfere with the right to education.[292]

Taking CESCR's assertion that such an obligation 'requires States parties to refrain from interfering directly or indirectly with the enjoyment of the Covenant rights by persons outside their territories' as well as the Maastricht Principles interpretation that State responsibility is incurred when such interference is 'a foreseeable result of their conduct,' sanctions restricting access to certain digital resources, if reasonably

[286] ibid, para 37 and 89
[287] see GC 13, para 6(b)(ii)
[288] GC 13, para 6
[289] ICESCR Article 2(1)
[290] De Schutter et al, p. 1094
[291] Narula, p. 128
[292] If the obligation to provide 'international assistance and cooperation,' did emerge as a positive obligation of state parties, as some scholars have suggested, finding a violation on the part of sanctioning states may be more likely; see Narula, p. 128

foreseeable, might amount to a violation of the sanctioning states' obligations.[293] This would also be subject to the degree to which the effects of sanctions interfere with the right, which the Maastricht Principles suggest requires a 'real risk of nullifying or impairing the enjoyment' of the right to education.[294] A similar evaluation would be necessary for establishing state responsibility under the causation model described by in chapter 2.1.3. However, such an interpretation of a state's extraterritorial obligations under ICESCR has not been tested under the treaty body and the sources relied on are not of the highest authority. Still, given that the obligation to provide international assistance and cooperation towards the realization of the right is recognized by Western states as at least a moral obligation, and given that providing such educational resources would likely support the goals of many sanctions regimes, it does seem that states might be receptive to arguments that states have a moral responsibility to facilitate access to such resources under the ICESCR. As a final note, considering that many digital educational resources are privately owned, the respective companies should adhere to their responsibilities to respect human rights under the UNGPs in responding to sanctions and the host states should exercise effective due diligence to avoid facing indirect attribution of extraterritorial violations of the right to education.[295]

3.2.2 Benefits of Scientific Progress

Each of the previous sections considers the human rights impact of technology sanctions on the basis of the role that restricted technologies have in exercising a particular right, whether it be freedom of expression, assembly and association, the right to privacy, or the right to education. Thus, the finding of a legal obligation to provide access to or refrain from interfering with access to certain technologies rests on their particular value and relative importance within the content of the rights protections. This section considers whether under the right to enjoy the benefits of scientific progress, an argument could be made for the obligation to protect access to such technologies outright. Enumerated in both the UDHR (Article 27) and ICESCR (Article 15), the right to enjoy the benefits of scientific progress and its applications was

[293] Maastricht Principles, Principle 13
[294] ibid
[295] Coursera's decision to make their product available in Syria following General License No. 11A suggests that the company is maintaining an awareness of changes to the sanctions policy which allow it to provide its products and services; see Kehl 2014

clearly considered an important element of the fundamental rights guaranteed to all, likely due to science's contributions to human and societal development.[296] Unfortunately, perhaps due to its vague formulation in law and lack of established jurisprudence, the right has largely been neglected by human rights bodies and legal scholars.[297] However, it is receiving renewed attention as the human rights community seeks to strengthen the link between science and human rights given the ever more dominant role that science and technology play in the exercise of nearly all enumerated rights.[298] In this way, the right to the benefits scientific progress could be viewed as a means of addressing situations where it is unclear what the precise content of other existing rights might be in the digital age.[299]

While there is no authoritative interpretive text to ICESCR Article 15, a number of legal experts such as Audrey Chapman[300] and the Special Rapporteur in the field of cultural rights, have cautiously attempted to articulate its content. Considering these interpretations alongside the text of Article 15 itself, it would appear that the right generally establishes that the benefits of science and its applications (i.e. technology) should be accessible to everybody, and thus broadly disseminated.[301] The Special Rapporteur in the field of cultural rights has also asserted that the 'benefits' of science includes 'the scientific process, its methodologies and tools,'[302] which in the context of digital technologies would seem to encompass both the technology products as well as the software and related tools necessary to engage in the process of technology development itself. Additionally, Article 15(4) provides that State Parties recognize the benefits of encouraging and developing international contacts and cooperation in the scientific field, thus giving the right an international, extraterritorial dimension. Further, advances in science require 'require freedom of inquiry and free circulation of ideas and research findings,' which may imply non-interference with other rights including freedom of thought, expression, movement, and association.[303] As Chapman, one of the

[296] UNDP, "Human Development Report 2001: Making New Technologies Work for Human Development," (OUP, 2001), p. 28
[297] Audrey Chapman, "Towards an Understanding of the Right to Enjoy the Benefits of Scientific Progress and Its Applications," (Journal of Human Rights, 2009), p. 1
[298] Coccoli, p. 238
[299] ibid
[300] see note 297
[301] ICESCR Article 15(1)(b); see also A/HRC/20/26, para 21
[302] A/HRC/20/26, para 24
[303] ibid; see also Report of the Experts' Meeting on the Right to Enjoy the Benefits of Scientific Progress and its Applications, (UNESCO, 2009), p. 17

leading legal experts on the right to the benefits of scientific progress argues, 'any limitation of or interference with these rights would constitute a violation of the right to enjoy the benefits of scientific progress.'[304] As such, given the more international framing of the ICESCR by comparison to the strict understanding of jurisdiction under the ICCPR, in the case of the effects of technology sanctions on the right to freedom of expression or the right to privacy for instance,[305] Article 15 may provide a more solid legal basis for establishing a breach of extraterritorial state obligations on the part of the sanctioning state.

Many if not all of the effects of technology sanctions noted in previous sections of this analysis implicate the right to the benefits of scientific progress as it is described here. For instance, access to a free and open Internet, the ability to use online platforms to access and share information, and access to encryption tools, amount to applications of scientific progress in and of themselves and enable the sharing of information and resources *about* scientific progress where it would otherwise be denied.[306] Specific tools like the Samsung, Apple, and Google app stores, which have been or continue to be blocked in states targeted by US sanctions,[307] are some of the largest repositories of mobile technologies and tools and are used globally to access and disseminate the majority of mobile ICT tools in existence. Platforms such as Gitlab, GAE, Google Cloud Platform, AWS, and Digital Ocean, frequently used by developers and technology companies, have also been made inaccessible by US technology sanctions, further limiting the ability of individuals within sanctioned states to participate in the ICT economy and access or develop modern ICT products and resources.[308] Other sectors, such as health and humanitarian aid, have been affected by technology sanctions in Syria, such as the WHO-reported incident of a CT scanner that required special license for an US-made component which took 6 months to receive, depriving patients of potentially life-saving technology.[309] Humanitarian actors in Syria also report that US-sourced radio

[304] Chapman, p. 17
[305] see Chapter 3.1
[306] A/HRC/29/32, para 24
[307] In a 2018 official statement, Apple explained that, 'Under the US sanctions regulations, the App Store cannot host, distribute, or do business with apps or developers connected to certain US embargoed countries;' see Jacob Kastrenakes, "Apple appears to have totally cut off Iran from the App Store," (The Verge, Mar 15, 2018)
[308] see note 164
[309] see A/HRC/39/54/Add.2, para 43

telecommunications tools which are standardized across the UN had been affected by sanctions, causing delays in their work as they sought proper licensing to bypass sanctions.[310]

In the absence of any authoritative legal interpretation of right to the benefits of scientific progress and established jurisprudence, it is difficult to say what forms of scientific knowledge and technologies are guaranteed under the right and to what extent states are obligated to ensure access to them, both within their own borders and extraterritorially.[311] However, it is likely, given the growing importance of the right to the benefits of scientific progress in the modern world, that some of these persisting questions will be answered in the future, either through a CESCR general comment or via individual complaints. Until such developments occur, in evaluating whether the effects described above as well as in previous sections of this analysis amount to a violation of the sanctioning state's legal obligations under the right to enjoy the benefits of scientific progress, it will be necessary to consider the content of Article 15 in light of recent interpretations, which largely infer obligations from the content of other more established ICESCR rights.

As with all other human rights, states are considered to have obligations to respect, protect, and fulfill the right to enjoy the benefits of scientific progress. Under the obligation to respect, states must ensure that their laws, policies, and actions do not interfere with the exercise of the right, nor those freedoms indispensable to its advancement.[312] The obligation to protect includes a positive duty to prevent and mitigate possible infringements of fundamental rights linked to the misuse of scientific and technological developments by third parties,[313] while the obligation to fulfill requires positive measures to promote the 'development and diffusion of science and technologies.'[314] As noted previously, Article 15(4) as well as the Article 2(1) of ICESCR may also provide for an extraterritorial dimension to the right. In the context of the right to water, this extraterritorial dimension is understood by CESCR to include a negative obligation to refrain from depriving another country of the ability to realize the right within its own borders.[315] A similar obligation may also apply with respect to Article 15, and would have particular importance in the context of

[310] ibid, para 47
[311] Chapman, p. 1
[312] UNESCO (2009), p. 17
[313] United Nations, Declaration on the Use of Scientific and Technological Progress in the Interest of Peace and for the Benefit of Mankind. General Assembly. Resolution 3384, (1975), Art. 6
[314] UNESCO (2009), p. 17
[315] see CESCR General Comment 15, para 31

technology sanctions, which may deprive access to ICT products and resources protected under Article 15. Chapman also argues that there may be a positive extraterritorial obligation under Article 15 for developed countries in particular to 'furnish assistance in the fields of science and technology and to enable access to essential knowledge and technologies,'[316] noting however that what this encompasses will need to be elaborated.[317] She completes this line of thought by asking whether there might be technologies 'so essential to the welfare of the inhabitants of particular countries,' that there should be a collective right of access from the international community?[318]

Some have answered this question in the affirmative when it comes to modern ICTs and the Internet, including the Special Rapporteur in the field of cultural rights who claims that Article 15 should 'be understood as including a right to have access to and use ICTs and other technologies in self-determined and empowering ways.'[319] She also asserts that 'with the Internet emerging as a critical platform for scientific and cultural flows and exchanges, freedom of access to it and maintaining its open architecture are important for upholding the right of people to science and culture.'[320] A similar understanding of the right was advocated at a 2007 UNESCO experts' meeting, with one participant arguing that the right to the benefits of scientific progress 'should be used as a means to ensure the spread of ICTs and combat exclusion from non-access to the Internet.'[321] Finally, asserting both negative and positive extraterritorial obligations under the right with respect to modern ICTs, Chapman has also posited that state parties must 'refrain from erecting barriers to scientific communication and collaboration across borders,' and facilitate the transfer of knowledge resources and products.[322]

Given the expansive nature of the technology sanctions discussed previously in this chapter and the above-recognized importance of the types of knowledge and tools restricted by sanctions for the enjoyment of the right to the benefits of scientific progress, it seems possible that sanctions could be held to interfere with the right for individuals in the targeted state. Regardless of the availability of alternative tools and

[316] citing CESCR General Comment 12, para 38-40
[317] Chapman, p. 30
[318] ibid
[319] A/HRC/20/26, para. 19
[320] A/HRC/20/26, para 36
[321] see UNESCO, "Experts' meeting on the Right to Enjoy the Benefits of Scientific Progress and its Applications," (2007), Session 6
[322] Chapman, p. 28

software, restricting access to numerous major cloud computing platforms, site developers, and app stores substantially interferes with both the scientific process of technology development and access to its products. Further, given the recognition of the unique importance of ICT tools within the scope of ICESCR Article 15, it would appear that access to such tools would be broadly protected and their protection may even be considered a core obligation under the right.[323] Particularly given that access to these scientific applications is often already heavily restricted by the territorial state in the case studies examined, imposing technology sanctions within these repressive contexts where global ICT tools are of the utmost value, has substantial adverse impacts on the ability of individuals to enjoy the benefits of scientific progress. As such, the state imposing technology sanctions of the type described might be said to interfere directly or indirectly[324] with the international transfer of and access to scientific knowledge and technologies within the targeted state in substantial and likely foreseeable ways. Thus, under the framework asserted by the Maastricht Principles as well as the causation model of extraterritorial jurisdiction established by the IACtHR, technology sanctions may violate a sanctioning state's negative extraterritorial obligations to respect the right to the benefits of scientific progress.[325]

Considering that Article 15(4) also specifically enumerates the benefits of international cooperation and assistance in addition to its status as a general obligation of state parties under Article 2(1), it would appear that this component of the right has special significance, perhaps amounting to a positive obligation on state parties to allow for and facilitate the transfer of science and technology to foreign states.[326] As discussed previously, the nature of extraterritorial positive obligations is likely dependent on the degree of control exercised in the foreign state or the degree to which the state exercises 'decisive influence' over this right.[327] Given that many technology companies are centralized in a few select counties, particularly the US, certain states may be in a position of decisive influence with respect to the right to enjoy the benefits of scientific progress, and may have positive obligations to facilitate access to these tools extraterritorially.[328] Thus,

[323] Maastricht Principles, Principle 22 asserts that sanctions should particularly avoid targeting those resources essential to the core obligations of the right in the targeted state; see chapter 2.1.2
[324] see Maastricht Principles, Principles 19 and 20
[325] see chapter 2.1.2 and 2.1.3
[326] Chapman, p. 28
[327] Maastricht Principles, Principle 9(c)
[328] ibid

imposing broad technology sanctions may be seen as a breach of such obligations under Article 15 amounting to a violation. Additionally, as with all previous rights discussed in the context of technology sanctions, it is often the internal decision-making of companies like Google, Apple, and others in response to sanctions which directly result in the deprivation of access to certain products and services.[329] However, based on its positive obligation to protect the right to the benefits of scientific progress, a sanctioning state might be required to revise sanctions regimes to explicitly permit private actors to export certain technologies or exert direct influence over them to ensure their compliance with human rights under its due diligence obligations.[330] If it does not take such measures, and in light of the broad scope of restrictions on the right to enjoy the benefits of scientific progress described above, it seems very likely that such interferences with the right may be indirectly attributable to the state, even if they are the result of a private company's actions. Regardless, overcompliance on the part of companies, such as has been reported with LinkedIn's decision to delete all Syrian users from the platform,[331] exacerbates the effects of technology sanctions on the rights of individuals in the target state, in particular with respect to the right to the benefits of scientific progress. Thus, further elaboration as to the content of Article 15 should include discussion of the significant role of private actors in realizing this right and provide specific guidance as to what is required of multinational corporations under their responsibility to respect the right.

4. Conclusion

The above analysis as to whether states may be held legally responsible for the impact of technology sanctions on human rights illustrates the difficulty of applying the human rights framework to these types of situation. The uncertain nature of more flexible models of extraterritorial jurisdiction, limited jurisprudence establishing the content of rights in light of rapid ICT developments, and the relatively untested argument for indirect attribution of human rights violations on the basis of due diligence, mean that much of this

[329] Both companies recently determined in 2019 that GL D-1, which applies to US sanctions in Iran, does not authorize US companies to host Iranian-developed apps; see Center for Human Rights in Iran, "Millions of iPhone Users Unable to Use Iranian Apps Due to Apple Certificate Revocation," (March 1, 2019)
[330] Chapman, p. 18
[331] The company later admitted overcompliance and reinstated service to Syrian users; see Jillian York, "LinkedIn Alienates Syrian Users: Why Now?" (HuffPost, May 25 2011)

analysis is speculative, based on in-progress legal evolutions. However, what is demonstrated clearly is that technology sanctions can have significant impact on the exercise and protection of human rights in the targeted state. Building on the understanding that 'the same rights that people have offline must also be protected online,'[332] more recent interpretations of human rights increasingly recognize the essential nature of digital technologies to the way that these rights are protected and exercised in the modern world. Thus, there is solid basis for arguing that intentionally depriving individuals of access to ICT technologies may amount to an interference with the rights examined above.[333]

Yet, establishing interference with a right does not automatically amount to state responsibility. This is particularly the case given the emergence of digital technologies and their importance across global societies, which allow states to exert substantial influence over human rights in a foreign state, absent any physical presence or effective control.[334] As demonstrated in this paper, the failure of the human rights law framework to adapt to these new scenarios may lead to an accountability gap, wherein states can seriously affect the enjoyment of human rights in a foreign state through measures such as technology sanctions without incurring any legal responsibility. Thus, dominant models of extraterritorial jurisdiction likely need to be replaced or reinterpreted so that they may better account for state actions with extraterritorial impact, particularly with respect to civil and political rights obligations under the ICCPR which are more strictly limited by territorial control and jurisdiction. Support for the impact model of extraterritorial jurisdiction under HRC General Comment 36 as well as the IACtHR's advancement of the causation model,[335] both indicate a growing recognition by international human rights bodies of the need to reevaluate existing bases of extraterritorial jurisdiction, which may increase the likelihood of state responsibility for acts like the imposition of technology sanctions resulting in adverse extraterritorial impact on human rights.

Given the ICESCR's lack of a jurisdictional requirement and general obligation to provide international assistance and cooperation towards the realization of the enumerated rights, it could be considered a more appropriate means of accounting for actions with extraterritorial human rights effects where effective control

[332] A/HRC/RES/32/13
[333] Peacock, p. 6
[334] see Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (vol 56, HIJL 2015)
[335] see chapter 2.1.1 and 2.1.3

is absent. This is supported by the fact that previous efforts to advance state responsibility for the extraterritorial human rights impact of sanctions, such as CESCR General Comment 8, have centered around economic, social and cultural rights.[336] Additionally, as some have considered,[337] the oft-neglected right to the benefits of scientific progress could take on unique importance in the digital era and provide a basis for addressing the control over ICTs that mostly Western states and the technology companies under their jurisdiction assert globally. However, the lack of attention given to establishing the nature of extraterritorial obligations under the ICESCR as well as the lack of a general comment or relevant jurisprudence on Article 15, hinder the application of this body of rights to the matter of technology sanctions.

Thus, despite strong condemnations of the 'egregious human rights impact' of economic sanctions from the current Special Rapporteur on the matter, and his assertion that 'such measures are clearly illegal and their source countries should be called to account,' there is narrow possibility within the *existing* human rights framework for such accountability to take place with respect to technology sanctions. The Maastricht Principles and CESCR General Comment 8[338] make similar statements to the Special Rapporteur, holding that sanctions regimes which do not seek to minimize the negative impact on human rights as much as possible may be considered unlawful.[339] However, as demonstrated, this type of claim is relatively unfounded when it comes to the broad and serious restrictions on technology imposed by US sanctions regimes in Iran, Syria, and Sudan, exposing the limitations of the way that state obligations have typically been understood under international human rights law. It is the hope of this author that greater recognition of the serious extraterritorial impact that policies like technology sanctions can have on human rights, and the legal challenges presented by such situations, will drive forward the effort to begin to resolve some of these outstanding issues with the existing human rights law framework and provide a more effective route to state responsibility.

[336] see CESCR General Comment 8 and Maastricht Principles, Principle 22
[337] see Coccoli and Chapman
[338] see Chapter 2.1.2
[339] see also A/HRC/36/44, Annex I, para 7

Bibliography

Cases:

Al-Skeini v. Sec'y of State for Def. (Judgement), App. No. 55721/07, 2011 Eur. Ct. H.R

Appleby v. United Kingdom, Application no. 44306/98 (2003.5.6), ECtHR (Judgment)

Autronic AG v. Switzerland, ECtHR, App. No. 12726/87 (1990)

Bankovic et al. v. 17 NATO Member States App no. 52207/99 (ECtHR, 12 December 2001)

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), ICJ, Judgement, 19 December 2005

Communication No. 1539/2006 (Munaf v. Rom.), adopted 30 July 2009, U.N. GAOR, Hum. Rts. Comm., 96th Sess., Annex ¶ 14.2, U.N. Doc. CCPR/C/96/D/1539/2006 (2009).

Cumhuryiet Vafki and others v. Turkey, ECHR 10.08.2013

IACtHR Advisory Opinion OC-23/17, para 104(h)

Issa and Others v. Turkey, no. 31821/96

Frasila and Ciocirlan v. Romania App no 25329/03 (ECtHR, 10 May 2012)

Öcalan v. Turkey [GC], no. 46221/99, § 91, ECHR 2005-IV

Jaloud v the Netherlands, App. No. 47708/08, 2014

Jankovski v. Lithuania, Application no. 21575/08 of 17 January 2017

Kalda v. Estonia, Application no. 17429/10 of 19 January 2016

Klass and Others v. Germany, ECtHR, Application no. 5029/71, 6 September 1978

Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, ICJ Advisory Opinion, 9 July 2004

Liberty and Others v. the United Kingdom, ECtHR Application no. 58243/00, 1 July 2008

Loizidou v. Turkey (Judgment), App. No. 15318/89, 310, ECtHR, (1995)

Pad and Others v Turkey, App. No. 60167/00, 2007

Ricci v. Italy, ECHR 10.08.2013 - 30210/06

Sergio Euben Lopez Burgos v Uruguay, Communication No.R.12/52, (A/36/40)

Threat or use of nuclear weapons, ICJ Reports, 1996 (Advisory Opinion)

Velasquez Rodriguez v Honduras, Judgement, 29 July 1989, Series C No. 4, 28 ILM 291

Yildirim v. Turkey, App no 3111/10 (ECtHR, 18 December 2012)

Treaties:

Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms*, as amended by Protocols Nos. 11 and 14, 4 November 1950

Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969

UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999

UN General Assembly, *International Covenant on Economic, Social and Cultural Rights*, 16 December 1966, United Nations, Treaty Series, vol. 993

UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III)

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI

UN, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331

Other:

Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission on the Work of Its Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, at 43, UN Doc. A/56/10 (2001)

'Guiding Principles on Business and Human Rights: Implementing the United Nations' "Protect, Respect and Remedy" Framework,' UN Doc. A/HRC/17/31 (21 March 2011)

International Commission of Jurists (ICJ), Maastricht Guidelines on Violations of Economic, Social and Cultural Rights, 26 January 1997

Maastricht Principles on Extraterritorial Obligations of States in the Area of Economic, Social and Cultural Rights, (adopted Sept. 28, 2011).

UN General Assembly, Promotion and protection of the right to freedom of opinion and expression, 10 August 2011, A/66/290

UN General Assembly, Promotion and protection of the right to freedom of opinion and expression, 4 September 2013, A/68/362
UN General Assembly, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 29 August 2017, A/72/370
UN Human Rights Council, Human rights and unilateral coercive measures, 3 Oct 2014, A/HRC/RES/27/21
UN Human Rights Council, Proceedings of the workshop on the various aspects relating to the impact of the application of unilateral coercive measures on the enjoyment of human rights by the affected populations in the States targeted, 24 June 2013, A/HRC/24/20
UN Human Rights Council, Report of the Special Rapporteur in the field of cultural rights, Farida Shaheed, "The right to enjoy the benefits of scientific progress and its applications," A/HRC/20/26 (2012)
UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights on his mission to the Syrian Arab Republic, 11 September 2018, A/HRC/39/54/Add.2
UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 30 August 2018, A/HRC/39/54
UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 26 July 2017, A/HRC/36/44
UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, on his mission to the Sudan, 4 August 2016, A/HRC/33/48/Add.1
UN Human Rights Council, Report of the Special Rapporteur on the negative impact of unilateral coercive measures on the enjoyment of human rights, 10 August 2015, A/HRC/30/45
UN Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, 24 April 2013, A/HRC/23/39
UN Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet: resolution / adopted by the Human Rights Council, 18 July 2016, A/HRC/RES/32/13
UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 28 May 2019, A/HRC/41/35
UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 22 May 2015, A/HRC/29/32
UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 17 April 2013, A/HRC/23/40
UN Human Rights Council, Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Addendum, Communications to and from Governments, 16 May 2011, A/HRC/17/27
UN Human Rights Council, Resolution adopted by the Human Rights Council on 23 March 2017, The right to privacy in the digital age, 7 April 2017, A/HRC/RES/34/7
UN Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, 17 May 2019, A/HRC/41/41
UN Human Rights Council, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, 26 July 2018, A/HRC/38/34
UN Human Rights Council, Report of the Special Rapporteur on the right to privacy, 27 February 2019, A/HRC/40/63
UN Human Rights Committee (HRC), General comment no. 31 [80], The nature of the general legal obligation imposed on States Parties to the Covenant, 26 May 2004, CCPR/C/21/Rev.1/Add.13
UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988
UN Human Rights Committee (HRC), General comment no. 34, Article 19, Freedoms of opinion and expression, 12 September 2011, CCPR/C/GC/34
UN Committee on Economic, Social and Cultural Rights (CESCR), General Comment No. 8: The relationship between economic sanctions and respect for economic, social and cultural rights, 12 December 1997, E/C.12/1997/8

U.S. Dep't of State, Pub. Notice 8086, State Department Sanctions Infor-mation and Guidance (Nov. 8, 2012).
U.S. Dep't of Treas., General License Related to Personal Communication Services (2010)
U.S. Dep't of Treas., General License D-1 with Respect to Certain Services, Software, and Hardware I ncident to Personal Communications (2014).

Books:
Coomans F and Künnemann R (eds.), *Cases and Concepts on Extraterritorial Obligations in the Area of Economic, Social and Cultural Rights*, (Intersentia, 2012).
Cortright D and Lopez G, "Smart sanctions : targeting economic statecraft," (Rowman & Littlefield, 2002).
Crawford J, *The International Law Commission's Articles on State Responsibility: Introduction, Text, and Commentaries* (CUP, 2002).
Gibney M and Skogly S, *Universal human rights and extraterritorial obligations*, (Philadelphia : University of Pennsylvania Press, 2010).
Happold M and Eden P, *Economic sanctions and international law*, (Oxford: HART Publishing, 2019).
Langford M, Vandenhole W, Scheinin M, & Van Genugten W. (Eds.), *Global Justice, State Duties: The Extraterritorial Scope of Economic, Social, and Cultural Rights in International Law*, (Cambridge University Press, 2012).
Milanovic M, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy, (Oxford : Oxford University Press, 2011).
Moeckli D, Shah S and Sivakumaran S (eds.) International human rights law (3rd edn. OUP 2014)
Peacock A, *Human rights and the digital divide*, (1st edn., London Routledge, 2019).
Ronzitti N (Eds.), *Coercive Diplomacy, Sanctions and International Law*, (Brill Nijhoff , 2016)
Skogly S, Beyond National Borders: States' Human Rights Obligations in International Cooperation (Antwerpen, Intersentia, 2006)
Ziccardi G, *Resistance, Liberation Technology and Human Rights in the Digital Age,* (Springer Netherlands, 2013).

Articles:
Bonnitcha J and McCorquodale R, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights," *European Journal of International Law*, (Volume 28, Issue 3, August 2017), p. 899–919.
Center for Human Rights in Iran, "Guards at the Gate: The Expanding State Control Over the Internet in Iran," (2018).
Chapman A, "Towards an Understanding of the Right to Enjoy the Benefits of Scientific Progress and Its Applications," (Journal of Human Rights, 8:1, 2009), 1-36.
Coccoli J, "The Challenges of New Technologies in the Implementsting of Human Rights: an Analysis of Some Critical Issues in the Digital Era," (Peace Human Rights Governance, 2017), 223-250.
Deeks A, "Does the ICCPR Establish an Extraterritorial Right to Privacy?" Lawfare, (14 Nov 2013).
De Schutter O et al, '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, at 1084-1171
Herr R.E., "Can human rights law support access to communication technology? A case study under Article 10 of the right to receive information," (Information & Communications Technology Law, 22:1, 2013), 1-13.
"Joint submission to the Universal Periodic Review of the Islamic Republic of Iran by ARTICLE 19 and Access Now," (April 4, 2019).
Kannis E, "Pulling (Apart) the Triggers of Extraterritorial Jurisdiction, 40 U.W. AUSTL. L. REV. 221, 2015), 243.
Kehl D, Maurer T & Phene S, "Translating Norms to the Digital Age: Technology and the Free Flow of Information under U.S. Sanctions," (NEW AM. FOUND. 12, 4 Dec. 2013).
Mehta P, "Sanctioning freedoms: U.S. sanctions against Iran affecting information and technology companies," University of Pennsylvania Journal of International Law, 37(2), 763-812.
Milanovic M, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (vol 56, HIJL 2015).

Møgster D, “Towards Universality: Activities Impacting the Enjoyment of the Right to Life and the Extraterritorial Application of the ICCPR,” (EJIL Talk!, 27 Nov 2018)
Langford M et al (eds.), *Global Justice, State Duties. The Extraterritorial Scope of Economic, Social and Cultural Rights in International Law*, (Cambridge University Press, 2013).
Peksen, D, Better or Worse? The Effect of Economic Sanctions on Human Rights. *Journal of Peace Research, 46*(1), 2009, 59-77
Peksen D, “Coercive Diplomacy and Press Freedom: An Empirical Assessment of the Impact of Economic Sanctions on Media Openness,” *International Political Science Review*, (31(4), 2010), 449-469.
Peksen D. & Drury A.C. Economic Sanctions and Political Repression: Assessing the Impact of Coercive Diplomacy on Political Freedoms, (Hum Rights Rev, Vol. 10, Issue 3, 2009), 393.
Petrossian V, “Iran Back in the Firing Line,” (36 MIDDLE E. ECON. DIG. 2, 2, Dec. 4, 1992)
Report of the Experts' Meeting on the Right to Enjoy the Benefits of Scientific Progress and its Applications, (UNESCO, 2007).
Report of the Experts' Meeting on the Right to Enjoy the Benefits of Scientific Progress and its Applications, (UNESCO, 2009).
Schulz W and Hoboken J, “Human rights and encryption,” (UNESCO 2016).
Tzevelekos V, ‘Reconstructing the Effective Control Criterion in Extraterritorial Human Rights Breaches: Direct Attribution of Wrongfulness, Due Diligence, And Concurrent Responsibility’, (Michigan Journal of International Law, 2015), 129.
UNDP, “Human Development Report 2001: Making New Technologies Work for Human Development,” (OUP, 2001).
United Nations, Declaration on the Use of Scientific and Technological Progress in the Interest of Peace and for the Benefit of Mankind. General Assembly. Resolution 3384, (1975)

News Reports:

Alimardani M and Pakzad R, “Silicon Valley preaches diversity and inclusion while excluding Iranians,” (Atlantic Council, 2019).
Bangi A, “The Impact of Sanctions Overcompliance on Iran,” (Iran Cyber Dialogue, 28 March 2016).
Bangi A and Saldias N, “Iranians Are Cut Off from the Internet Economy, Even with Lifted Sanctions,” (Vice, Oct 4 2016).
Center for Human Rights in Iran, “Millions of iPhone Users Unable to Use Iranian Apps Due to Apple Certificate Revocation,” (March 1, 2019).
Center for Human Rights in Iran, “More Iranians Forced to Rely on Unsafe Online Hosting After Amazon Ban,” (August 7, 2019).
Center for Human Rights in Iran, “Internet Freedom in Iran Will Benefit From Sanctions Relief,” (Jan 28 2016).
Cohn C and York J, “Stop the Piecemeal: Obama Administration Should Fully Free Communications Tech Exports to Syria (& Companies Should Help),” (EFF, September 26, 2011).
Cox J, “Slack Bans Iranian Academic Living in Canada Because of Sanctions,” (Vice, Dec 20 2018).
Cox J, “Google Gives Free Security Keys to Activists, But Not if You’re in Iran or Syria,” (Vice, April 26, 2019).
Franceschi-Bicchierai L and Koebler J, “Microsoft and Amazon Enable Censorship Circumvention Tools in Iran. Why Doesn’t Google?” (Vice, Jan 15 2018).
Frenkel S, “Iranian Authorities Block Access to Social Media Tools,” (NY Times, Jan. 2, 2018).
Groll E, “Why US sanctions are actually helping Iran crack down on protesters,” (Foreign Policy Jan 7, 2018).
Harrell P and Anderson C, “U.S. Sanctions Abet Iranian Internet Censorship,” (Foreign Policy, January 22, 2018).
Kastrenakes J, “Apple appears to have totally cut off Iran from the App Store,” (The Verge, Mar 15, 2018).
Kehl D, “US Government Clarifies Tech Authorizations under Iranian Sanctions,” (New America, Feb 12, 2014).
Kehl D and Maurer T, “Confusing Sanctions Are Aiding Government Repression,” (Slate, May 30 2013).
Knezevic M, “Why US sanctions are a blow to free expression,” (Index on Censorship, Jan 31 2014).
Mahmoudi F and Bashar F, “Tech Companies Are Complicit in Censoring Iran Protests,” (WIRED, 2018)

Marquis-Boire M, “Iranian anti-censorship software ‘Simurgh’ circulated with malicious backdoor,” (May 25, 2012).
Martin A, “Google faces calls to lift anti-censorship blocks in Iran,” (Sky News, January 2, 2018).
Sperber A, “In Sudan, Civil Society says It's Struggling to Work Around US Sanctions' Block on Tech,” (TechPresident, January 14 2014)
Tehran Times, “Some 64% of Iranians are internet users: report,” (January 11 2019)
York J, “LinkedIn Alienates Syrian Users: Why Now?” (HuffPost, May 25 2011)
York J and Carlson K, “Sudan Tech Sanctions Harm Innovation and Development: US Government and Corporations Must Act,” (EFF, June 26, 2014).
York J and Carlson K, “Export regulations on communication and educational technologies loosen for some sanctioned countries and not others—what gives?” (EFF, Feb 27 2014)