



[GW Law Faculty Publications & Other Works](#)

[Faculty Scholarship](#)

2022

Between a Rock and a Hard Place? ICT Companies, Armed Conflict, and International Law

Arturo J. Carrillo

George Washington University Law School, acarrillo@law.gwu.edu

Follow this and additional works at: https://scholarship.law.gwu.edu/faculty_publications

 Part of the [Law Commons](#)

Recommended Citation

46 Fordham J. Int'l L. (Forthcoming 2023)

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons. It has been accepted for inclusion in GW Law Faculty Publications & Other Works by an authorized administrator of Scholarly Commons. For more information, please contact spagel@law.gwu.edu.

Between a Rock and a Hard Place?*
ICT Companies, Armed Conflict, and International Law
Arturo J. Carrillo
George Washington University Law School

INTRODUCTION	2
I. PART ONE	6
A. THE OPERATION OF INTERNATIONAL LAW	6
B. THE APPLICATION OF INTERNATIONAL LAW	10
II. PART TWO	13
A. THE RUSSIAN-UKRAINIAN ARMED CONFLICT	15
B. INTERNATIONAL LAW, CYBERSPACE AND ARMED CONFLICT	19
III. PART THREE	24
A. CASE STUDY: RUSSIA’S WAR IN UKRAINE	24
B. ANALYSIS OF UKRAINE CASE STUDY	26
IV. CONCLUDING OBSERVATIONS	42

** I would like to thank the following persons for their input on previous drafts of this article: Jason Pielemeier, Jennifer Easterday, Evelyn Aswad, Jonathan Horowitz, etc. In addition, I am grateful to my research assistants Brooke Laing and Marco Guzman for their excellent support. Finally, I want to acknowledge the important role that my membership and participation in the Global Network Initiative (GNI) played in the development of this Article.

INTRODUCTION

Russia's invasion of Ukraine in February 2022 unleashed more than just the former's military might against the territory of its neighbor: it also set into motion a new era of power dynamics on the internet. Technology companies whose platforms and applications dominate the digital realm have found themselves in the eye of a geopolitical storm, besieged by government demands from all sides of the war unfolding in Ukraine to restrict the flow of, or provide access to, information.¹ This pressure to comply with State policies shaped by the international armed conflict between Russia and Ukraine, which is Europe's first since World War II, is exemplified by the European Commission's creation of a "crisis mechanism" through the enactment of the Digital Services Act ("DSA") in April of 2022.² This novel mechanism grants the Commission the authority, in times of crisis involving threats to public health or national security, to impose "a state of emergency on social media sites, search engines, and online marketplaces."³ It means that any of the 27 national governments comprising the EU may invoke the mechanism to censor content they deem a threat arising from the Ukraine conflict, such as propaganda for war or disinformation, something the EU had already acted to do.⁴ The EU's new expanded authority in this regard extends over all the world's major online platforms, including Meta, Google, YouTube, TikTok and Amazon.⁵

The DSA and its grant of authority to order information, communication and technology ("ICT") companies to regulate offending conduct online applies only to content that can be viewed in Europe.⁶ ICT companies must also respond to the stream of similar demands from the warring parties themselves: Russia and Ukraine.⁷ Unsurprisingly, the governments of both belligerents have been sending dueling requests to block access or restrict online content and telecommunications in a variety of forms. For example, Russia is pressuring big tech companies to censor social media posts and other information flows inside the country on top of already restricting domestic access to those sites, as it did with Facebook and Twitter.⁸ Outside of Russia, the Putin government has ordered such platforms to lift their restrictions on pro-Kremlin media outlets related to Ukraine.⁹ The Zelenskiy government in turn sent a letter to Internet Corporation for Assigned Names and Numbers ("ICANN") urging the non-governmental group to revoke the most common Russian internet domains and shut down the domain name system ("DNS")¹⁰ root

¹ Adam Satariano & Sheera Frenkel, *Ukraine War Tests the Power of Tech Giants*, NEW YORK TIMES, February 28, 2022, <https://www.nytimes.com/2022/02/28/technology/ukraine-russia-social-media.html?referringSource=articleShare>.

² Morgan Meaker, *Ukraine War Prompts Europe's New Emergency Rules for the Internet*, WIRED, April 25, 2022, <https://www.wired.com/story/europe-digital-services-act/>.

³ *Id.*

⁴ Natasha Lomas, *EU's Ban on Russia Today and Sputnik is Now in Effect*, TECH CRUNCH, March 2, 2022, <https://techcrunch.com/2022/03/02/eu-rt-sputnik-ban-live/>.

⁵ *See* Meaker, *supra* note 2.

⁶ *Id.*

⁷ Satariano and Frenkel, *supra* note 1.

⁸ Dan Milmo, *Russia Blocks Access to Facebook and Twitter*, THE GUARDIAN, March 4, 2022, <https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter>.

⁹ Adam Satariano, *Russia Intensifies Censorship Campaign, Pressuring Tech Giants*, NEW YORK TIMES, February 26, 2022, <https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html>.

¹⁰ "The Domain Name System (DNS) is the Internet's system for mapping alphabetic names to numeric Internet Protocol (IP) addresses like a phonebook maps a person's name to a phone number." What is a Domain Name and

servers in Russian territory.¹¹ In addition, Ukrainian authorities have for years sought to curtail inside the country the influx of Russian propaganda channeled through traditional and digital media, and now seek to do so more urgently than ever.¹²

In the face of such chaos – unprecedented in this digital dimension -- what’s an ICT company to do? How should responsible technology companies respond to government demands to regulate online content arising in and around international armed conflict, such as propaganda for war? How should they respond to similar demands to provide access to personal data related to, or asserted to be justified by, the conduct of war? Is their decision-making at bottom just a “judgment call,” as some company executives would have it?¹³ Are tech companies simply required to “choose a side” when presented with competing demands by State parties to the conflict, as well as others that, while not active belligerents themselves, have expressly sided with one? Or is there a more principled approach to digital realm decision-making in the context of armed conflict? Fortunately, the answer to the last question is decidedly in the affirmative. As this Article will explain, ICT companies (and others) can and should draw upon existing normative frameworks to guide their actions in the midst of a geopolitical crisis like the one generated by the war in Ukraine.

Indeed, ICT companies in wartime, like in peacetime, should be guided by pre-existing frameworks of international legal norms designed precisely for this purpose. In times of peace, human rights law provides a series of principles organized into a widely-accepted framework for how private-sector businesses should conduct themselves when confronted with government abuses and related challenges.¹⁴ The UN Guiding Principles on Business and Human Rights, or UNGP as they are commonly known,¹⁵ have been adapted to the business models of ICT companies and applied to the protection of freedom of expression and privacy rights online, not least through the operation of multi-stakeholder initiatives like the Global Network Initiative (GNI).¹⁶ But human rights law was not designed for wartime, which is the bailiwick of international humanitarian law (IHL), also commonly referred to as the laws of armed conflict (LOAC).¹⁷ To quote John Ruggie, the former UN expert on business and human rights who oversaw the drafting of the UN Guiding Principles:

How Does DNS Work?, THOUSAND EYES, PART OF CISCO, <https://www.thousandeyes.com/learning/techtutorials/dns-domain-name-system> (last visited Jul 29, 2022).

¹¹ Jon Brodtkin, *Ukraine Asks ICANN to Revoke Russian Domains and Shut Down DNS Root Servers*, ARS TECHNICA, March 2, 2022, <https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea/>.

¹² Words and Wars: Ukraine Facing Ukraine Propoganda, UKRAINE WORLD, December 5, 2017, <https://ukraineworld.org/articles/infowars/words-and-wars-ukraine-facing-russian-propaganda>.

¹³ Satariano and Frenkel, *supra* note 1.

¹⁴ UN Guiding Principles, BUSINESS & HUMAN RIGHTS RESOURCE CENTRE, <https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/>.

¹⁵ United Nations Office of the High Commissioner of Human Rights, GUIDING PRINCIPLES ON BUSINESS AND HUMAN RIGHTS, (2011),

https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

¹⁶ Global Network Initiative, About, GLOBAL NETWORK INITIATIVE, <https://globalnetworkinitiative.org/> (last visited Jul 6, 2022).

¹⁷ War & Law, INTERNATIONAL COMMITTEE OF THE RED CROSS, <https://www.icrc.org/en/war-and-law> (last visited Jul 6, 2022).

[c]onflict zones are [...] problematic because nobody can claim that the human rights regime, as it is designed, can possibly function in a situation of extreme duress for the host state. [Accordingly,] in situations of [armed] conflict, companies themselves ought to be looking to international humanitarian law to make sure that they do not find themselves either directly or indirectly contributing to violating IHL provisions or end up complicit in IHL violations.¹⁸

Thus, a normative framework *does* exist in answer to the touchstone question of how an ICT company should conduct itself in times of war *vis-à-vis* the actions of governments who are belligerents. The rub is that we must look to at least two different bodies of international law – human rights and humanitarian law – to understand what that framework consists of, and how it operates in practice. That is what I propose to do in this Article. Before proceeding, however, a caveat is in order. The focus of my analysis is on the legal obligations of *States*, because under the UNGP framework, ICT companies are expected to respect those obligations when faced with governments demands to the contrary.¹⁹ At the same time, however, if “national laws, regulations and policies do not conform to international standards, ICT companies should avoid, minimize, or otherwise address the adverse impact of government demands, laws, or regulations, and seek ways to honor the principles of internationally recognized [norms] to the greatest extent possible.”²⁰ My emphasis on the former point in no way minimizes the dictates of the latter.

The war in Ukraine has framed a unique set of opportunities for protecting fundamental human rights and values on the internet. In late April 2022, soon after the EU’s enactment of the DSA, the United States announced that it and 60 other State “partners” were assuming a series of political commitments to advance “a positive vision for the Internet in the face of [...] global challenges presented by the 21st century.”²¹ This vision expressly includes a commitment to foster and protect “privacy” and “respect for human rights” online.²² Christened the *Declaration for the Future of the Internet*, this manifesto calls for participating nations to work towards “a global Internet that advances the free flow of information” while “respecting each other’s regulatory autonomy [...] in accordance with [their] respective domestic laws and international legal obligations.”²³ In a response applauding the issuance of the Declaration, Microsoft’s Brad Smith pointedly raised the armed conflict in Ukraine as one of those 21st century challenges, highlighting that “our generation[’s]” ability to “act collectively to protect human rights on the internet” depends on our ability to build upon “one of the most important advances of the 20th

¹⁸ Vincent Bernard & Mariya Nikolova, *Interview with John G. Ruggie*, 94 INT. REV. RED CROSS 891–902, 892 (2012). <https://international-review.icrc.org/articles/interview-john-g-ruggie>.

¹⁹ Global Network Initiative, *GNI Principles on Freedom of Expression and Privacy*, 2, <https://globalnetworkinitiative.org/gni-principles/> (last visited Jul 8, 2022). (“The duty of governments to respect, protect, promote and fulfill human rights is the foundation of this human rights framework.”)

²⁰ *Id.*

²¹ FACT SHEET: United States and 60 Global Partners Launch Declaration for the Future of the Internet, (2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/28/fact-sheet-united-states-and-60-global-partners-launch-declaration-for-the-future-of-the-internet/?mkt_tok=MTM4LUVaTS0wNDIAAAGEEB16nnqeAmSdL7X91K8YfoTLscnfE1BY-uDNdJX9kywt7n9gYhamoiAh8HVPtUtNzQZ73uoLej_fs5XO6Q2QALGy9TMYFAZ0QqRajaGJTLRp.

²² *Id.*

²³ European Commission, *Declaration for the Future of Internet*, (2022), <https://digital-strategy.ec.europa.eu/en/library/declaration-future-internet>.

century, the proposition that governments must protect civilians even in a time of war” in accordance with the principles of the Fourth Geneva Convention.²⁴

What, then, does international law say to ICT companies besieged by government requests arising in the context of international armed conflict? How does a demarcation of international norms applicable to States under such wartime conditions serve to orient the policies and practices of ICT companies upon which belligerent and non-belligerent governments place their demands, including in the scenarios mentioned above? Under what circumstances can international armed conflict justify government censorship or data access demands that would otherwise be inconsistent with the States’ obligations under human rights law? Finally, what legal or normative sources operate in such situations, and how can ICT companies use them to evaluate specific government demands and restrictions based on or justified by the conditions arising from a war between nations?

In this Article, I will address these and related questions to provide at least preliminary answers to most of them. It is divided into four Parts. I begin in Part I by examining *when* and *how* the relevant bodies of international law apply to and during armed conflict between States generally. This initial Part introduces the discussion of a critical issue: the overlap and interplay between the laws of war and human rights law where both are in effect, with particular reference to the situation of Ukraine. In Part II, I take a step back to explain *why* ICT companies must engage with IHL before describing *how* they can do so. With respect to the latter, I return to the first round analyses of “real-world” scenarios arising from the armed conflict in Ukraine to focus first on Russia, and then on the European Union. Part II concludes with an overview of the broader international law panorama within which all these scenarios are taking place. Part III takes a deeper dive into more detailed factual scenarios involving the protection of digital rights in war zones specifically. I conclude in Part IV with observations *inter alia* on the critical role of multi-stakeholder initiatives (MSIs) in promoting a greater understanding and more effective implementation of the international framework outlined herein.

As it turns out, international law provides the parameters required to responsibly navigate a path between the “rock and a hard place” this dilemma reflects. Accordingly, this Article does not just demarcate the landscape of States’ obligations under international law in times of war with respect to digital rights, which is a starting point for ICT executives concerned about enabling government abuses. It also offers normative guidance to companies as well as other stakeholders operating in the digital realm when addressing competing demands that impact fundamental rights from belligerent and non-belligerent parties alike. One thing this Article will *not* do is engage with the related but distinct questions posed by the use of digital technologies to wage war, specifically through cyber operations that amount to “attacks” or hostile acts under the

²⁴ Brad Smith, *A Vital Step at a Critical Moment: The Declaration for the Future of the Internet*, MICROSOFT ON THE ISSUES (2022), <https://blogs.microsoft.com/on-the-issues/2022/04/28/declaration-future-internet-cybersecurity-governance/>. See also *infra* notes 215–225 and accompanying text; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287., https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.33_GC-IV-EN.pdf; see *infra* PART ONE: The Operation of International Law.

laws of armed conflict.²⁵ Russia’s cyber-attacks on Ukraine are indeed relentless.²⁶ Although very much a feature of modern “hybrid” warfare, the complex subject of military cyber operations and their implications for ICT companies operating in theaters of war is substantively different from the one addressed in this Article, and has been amply explored elsewhere.²⁷ What we are concerned with here is the conduct of governments relating to information and communications technologies used during armed conflicts for purposes *other* than as means and methods of warfare.²⁸ I will return to this important distinction later in the article.

I. PART ONE

In Ukraine like in other conflict zones, ICT companies seeking to adopt a principled position *vis-à-vis* a given government’s demands to censor information on the internet or interfere with privacy rights must first understand what duties international law imposes on that government. Only then can the company engage in an evaluation of whether said demands comport with the State’s legal obligations or not, a critical input into the company’s human rights due diligence calculus.²⁹ Accordingly, what follows is an abbreviated primer on the operation and application of international law as it relates to armed conflict between nations. In the first section of this Part, I examine the operation of State duties under international human rights law (IHRL) and IHL, as well as how those legal obligations apply to and in a particular country. In the second section we will address the concurrent application of these two bodies of law to better understand their interplay in theory and practice. While working through this framework I will reference the principal treaties and legal norms of IHRL and IHL in effect for the parties to the armed conflict in Ukraine, in addition to non-belligerent countries, like those comprising the European Union.

A. The Operation of International Law

International law emanates from a limited number of defined sources that include treaties, which are contractual agreements negotiated and subscribed by States, and customary international law (CIL), defined as norms that evidence a general practice among nations

²⁵ See Andy Greenberg, *The WIRED Guide to Cyberwar*, WIRED, August 23, 2019, <https://www.wired.com/story/cyberwar-guide/>; Jonathan Horowitz, *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, 24 AM. SOC. INT. LAW, np (2020), <https://www.asil.org/insights/volume/24/issue/11/cyber-operations-under-international-humanitarian-law-perspectives-icrc>; see also, Schmitt, Michael N., ‘Attack’ as a Term of Art in International Law: The Cyber Operations Context (September 7, 2012), <https://ssrn.com/abstract=2184833>; Gary Corn, *Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace* (December 16, 2017), in, *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare* (2018, Forthcoming), <https://ssrn.com/abstract=3089071>.

²⁶ Tom Burt, *The Hybrid War in Ukraine*, MICROSOFT ON THE ISSUES (2022), <https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/>.

²⁷ See, e.g., INTERNATIONAL COMMITTEE OF THE RED CROSS, *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions*, 26–29, https://www.icrc.org/sites/default/files/document/file_list/challenges-report_new-technologies-of-warfare.pdf (last visited Jul 6, 2022).

²⁸ See *infra* Part II(b) discussion.

²⁹ See Global Network Initiative, *supra* note 19, and accompanying text.

accepted as law.³⁰ It goes without saying that governments are bound to comply with their conventional (treaty-based) and CIL obligations to respect human rights and humanitarian law.³¹ And, as we shall see in the next two Parts, the obligations of companies in general, and of ICT companies in particular, is to ensure respect for those same fundamental norms by not enabling State violations of their IHRL and IHL obligations, or otherwise being complicit in such abuses.³² The starting place in either case is treaty law: what IHL and IHRL treaties have been ratified by the State in question and what is their scope of application?

While the rules governing treaty ratification and interpretation enshrined in the Vienna Convention on the Law of Treaties of 1969 (“VCLT”) will apply equally across the board to all treaties, the precise scope of application of *specific* treaties will depend on their express terms in this regard, and may vary.³³ As we shall see, this principle is critical to understanding how to navigate the overlap of IHL and IHRL in situations of armed conflict. Broadly speaking, the scope of application of each body of law is defined by two factors. The ground rules of international law like the Vienna Convention that apply to treaties are the first factor, most notably the edict in VCLT Article 26 that “every treaty in force is binding upon the parties [that have subscribed] to it and must be performed by them in good faith.”³⁴ The second factor governing a particular treaty’s scope of application are the express terms set out in the treaty itself for this very purpose. As with any legally binding agreement, treaties must define, among other things, the subject matter, geographic, and temporal contours of their application. Article 31(1) of the VCLT recognizes this when it states that “[a] treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.”³⁵

Let us take Ukraine as an example. Ukraine is a long-time State Party to the International Covenant on Civil and Political Rights (“ICCPR”) and the European Convention on Human Rights (“ECHR”);³⁶ it is also as a member of the Council of Europe (“COE”).³⁷ To simplify the exposition moving forward, I will focus on the ICCPR in the understanding that our discussion of how that treaty operates in relation to Ukraine and other States is representative of those countries’ conventional human rights obligations more broadly.

³⁰ Public International Law: A Beginner’s Guide - Sources of Law, LIBRARY OF CONGRESS RESEARCH GUIDES, <https://guides.loc.gov/public-international-law/sources-of-law> (last visited Jun 6, 2022) ; *see also*, Customary International Humanitarian Law, INTERNATIONAL COMMITTEE OF THE RED CROSS (2010), <https://www.icrc.org/en/document/customary-international-humanitarian-law-0>.

³¹ INTERNATIONAL LAW COMMISSION, *Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10, Art. 2 (2001) , https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf.

³² *See* Global Network Initiative, *supra* note 19 at 2, and accompanying text.

³³ Vienna Convention on the Law of Treaties, Jan. 27, 1980, 1155 U.N.T.S., 8 I.L.M. 679, https://legal.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf. [hereinafter “VCLT” or “Vienna Convention”]

³⁴ *Id.* at Art. 26.

³⁵ *Id.* at 31(1).

³⁶ *See* International Covenant on Civil and Political Rights, T.I.A.S. 94-1120, 999 U.N.T.S. 171, <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights> [hereinafter “ICCPR”]; European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, E.T.S. 5, 213 U.N.T.S. 221, https://www.echr.coe.int/documents/convention_eng.pdf [hereinafter “ECHR”]

³⁷ Council of Europe: 46 Member States, COUNCIL OF EUROPE, <https://www.coe.int/en/web/portal/46-members-states> (last visited Jul 6, 2022).

The VCLT is clear when it comes to the geographic scope of treaties in general terms: Article 29 states that “[u]nless a different intention appears from the treaty or is otherwise established, a treaty is binding upon each party in respect of its entire territory.”³⁸ The ICCPR in Article 2(1) expands on this scope by establishing that a “State Party to the [...] Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction” all the rights contained therein [emphasis added].³⁹ The ICCPR Human Rights Committee expounded on what is meant by “subject to its jurisdiction”, saying that the state has an obligation to respect and ensure ICCPR Rights to all within the “power or effective control”⁴⁰ of a state, alluding to a standard of extraterritorial jurisdiction also adopted by the European Court of Human Rights.⁴¹ At the same time, it is important to recognize that the ICCPR in Article 4 allows State parties to derogate from all but a handful of rights in a “time of public emergency which threatens the life of the nation and the existence of which is officially proclaimed” provided that such derogation is “not inconsistent with their other obligations under international law and do not involve discrimination.”⁴² Article 4 thus operates to narrow the scope of application of the ICCPR even further with respect to its subject matter (human rights protections) in times of existential threats to the State Party, such as was clearly the case with respect to Ukraine in the wake of Russia’s invasion.⁴³ We will return to this key point further below, not least because Ukraine has successfully derogated from its obligations under the ICCPR in this way.⁴⁴

The scope of application of the Geneva Conventions of 1949, the primary conventional sources of applicable law to the war in Ukraine, is qualitatively different. First and foremost, as defined in Article 2 common to the four Conventions, they will apply “to all

³⁸ VCLT, *supra* note 33, at Art. 29.

³⁹ ICCPR, *supra* note 36, at Art. 2(1) ; *see also*, GENERAL COMMENT NO. 31, THE NATURE OF THE GENERAL OBLIGATION IMPOSED ON STATES PARTIES TO THE COVENANT, CCPR/C/21/REV.1/ADD.13 ¶¶ 3 & 10 (2004), <https://www.unhcr.org/4963237716.pdf> (“[Art.2 (1)] means 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.”).

⁴⁰ ICCPR GEN. COMM. NO. 31, *supra* note 39.

⁴¹ For a summary of this line of jurisprudence, *see*, Isil Karakas & Hasan Bakirci, *Extraterritorial Application of the European Convention on Human Rights: Evolution of the Court’s Jurisprudence on the Notions of Extraterritorial Jurisdiction and State Responsibility*, in THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND GENERAL INTERNATIONAL LAW (2018), <https://oxford.universitypressscholarship.com/view/10.1093/oso/9780198830009.001.0001/oso-9780198830009-chapter-7>.

⁴² ICCPR, *supra* note 36, at Art. 4(1).

⁴³ *See*, What Happened on Day 8 of Russia’s Invasion of Ukraine - Catch Up on the Latest News of Ukraine, NEW YORK TIMES, March 3, 2022, <https://www.nytimes.com/live/2022/03/03/world/russia-ukraine#catch-up-on-the-latest-news-on-ukraine>;

GENERAL COMMENT NO. 29, ART. 4: DEROGATIONS DURING A STATE OF EMERGENCY, CCPR/C/21/REV.1/ADD.11 ¶ 3 (2001) <https://digitallibrary.un.org/record/451555?ln=en> (“The [ICCPR] requires that even during an armed conflict measures derogating from the Covenant are allowed only if and to the extent that the situation constitutes a threat to the life of the nation.”).

⁴⁴ UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *Update on the Human Rights Situation in Ukraine*, ¶5 (2022), https://www.ohchr.org/sites/default/files/2022-03/HRMMU_Update_2022-03-26_EN.pdf.

cases of declared war or of any other [international] armed conflict...”.⁴⁵ The Geneva Convention relative to the Protection of Civilian Persons in Time of War, known as Geneva Convention IV (GC IV) or the Civilians Convention, further stipulates that its unique scope of application applies similarly to “all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance.”⁴⁶ Finally, all four Geneva Conventions specify a category or categories of “protected persons” over whom they extend their respective safeguards; so, for example, Geneva Convention III covers prisoners of war, and is thus known as the POW Convention, while GC I and II address combatants rendered *hors de combat* on land and at sea, respectively.⁴⁷ These protections were expanded and updated in the Protocol Additional to the Geneva Conventions of 1949 relating to the Protection of Victims of International Armed Conflicts (1977), commonly referred to as Protocol I.⁴⁸ Ukraine, like Russia, is a long-standing State Party to the four Geneva Conventions, as well as Protocol I.⁴⁹

In short, international human rights treaties on the one hand, and those governing the laws of war on the other, each have very different scopes of application that must be considered separately when analyzing a scenario or situation of armed conflict on the territory of a State party. To better understand what that means in practice, we need look no further than the war in Ukraine, an international armed conflict between countries which, as noted, are subject to the four Geneva Conventions, Additional Protocol I, and customary international humanitarian law.⁵⁰ In other words, IHL applies by its own terms *exclusively* to the actions of the belligerents, Russia and Ukraine, the States at war with each other.⁵¹ More precisely, IHL will apply *wherever* hostilities are taking place and/or *wherever* the “protected persons” who are the objects of IHL’s safeguards may be. International human rights law meanwhile will apply only in the *territory* and *within the jurisdiction* of State parties, or under a state agent’s effective control -- belligerents or not -- and only to the extent that lawful derogation has not taken place there.⁵² In other words, the application of IHL is dictated more by the stipulated context and objects of its protections than by geography; IHRL on the other hand is bounded strictly by the State Party’s territory and jurisdiction.

⁴⁵ Classification - International Armed Conflict, RULAC GENEVA ACADEMY (2017), <https://www.rulac.org/classification/international-armed-conflict#:~:text=Common%20Article%20%20to%20the,recognized%20by%20one%20of%20them.>

⁴⁶ See Geneva Convention, *supra* note 24, at Art. 2.

⁴⁷ See Protected Persons, in HOW DOES LAW PROTECT IN WAR?, <https://casebook.icrc.org/glossary/protected-persons> (last visited Jul 6, 2022).

⁴⁸ Protocol Additional to the 1949 Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), June 8, 1977, 1125 U.N.T.S., 16 I.L.M. 1391, <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/470>.

⁴⁹ See Treaties, States Parties, and Commentaries - Ukraine, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=UA (last visited Jul 8, 2022). (G.C. Accession: Aug. 3 1954, Add. Pro. I Accession: Jan. 25, 1990); Treaties, States Parties, and Commentaries: Russian Federation, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=RU (last visited Jul 8, 2022). (G.C. Accession: Oct. 5, 1954, Add. Pro. I Accession: Sep. 29, 1989).

⁵⁰ See Treaties, States Parties, and Commentaries - Ukraine, *supra* note 49; Treaties, States Parties, and Commentaries: Russian Federation, *supra* note 49. And accompanying text.

⁵¹ See The Editors of Encyclopedia Britannica, *Belligerency: International Law*, ENCYCLOPEDIA BRITANNICA, <https://www.britannica.com/topic/belligerency> (last visited Jul 6, 2022).

⁵² See generally, Karakas and Bakirci, *supra* note 41; ICCPR GEN. COMM. NO. 31, *supra* note 39.

B. The Application of International Law

The foregoing clarifies the nature of Ukraine and Russia's obligations under international law so long as the war continues. But the devil is in the details, especially where IHL and IHRL are both in effect. Take Ukraine once again as an example. Because Ukraine is a belligerent, the laws of armed conflict apply fully to the conduct of hostilities there, as well as any other activities involving protected persons, such as POWs.⁵³ At the same time, the human rights framework emanating from the ICCPR and ECHR that operates normally in peacetime will continue to be in force throughout the country's territory, consistent with the scope of application of those treaties.⁵⁴ In this regard, the only allowance the ICCPR and ECHR make during wartime is the process of derogation, discussed in more detail below.⁵⁵ The point here is that so long as the conflict lasts, IHL and IHRL will apply *concurrently* throughout Ukrainian territory, raising challenges for ICT companies and others seeking to understand what rules pertain to particular scenarios arising in the context of the war there.⁵⁶

The concurrent application of IHL and IHRL in times of armed conflict is a common feature of the different bodies of norms that comprise international law in this context (the third such body is international criminal law).⁵⁷ But that does not make it any less contentious. The International Committee of the Red Cross (ICRC), the recognized authority in the field of international humanitarian law, describes their interrelation in the following terms:

Where contradictions exist between [IHRL and IHL] rules, some argue that IHL provisions always prevail, in every situation for which IHL has a rule or even through its allegedly qualified silence (e.g. by not referring to the freedom of press in the law of military occupation). Others, adopting an International Human Rights Law approach, argue that in any circumstance the rule providing the greatest level of protection must be applied. In [the] view of the [ICRC], it is preferable to adopt a case-by-case approach and to apply the more detailed rule, that is, that which is more precise vis-à-vis the situation

⁵³ International Law on the Conduct of Hostilities: Overview, INTERNATIONAL COMMITTEE OF THE RED CROSS (2010), <https://www.icrc.org/en/doc/war-and-law/conduct-hostilities/overview-conduct-of-hostilities.htm#:~:text=International%20law%20on%20the%20conduct%20of%20hostilities%20regulates%20and%20limits,human%20suffering%2C%20particularly%20among%20civilians>.

⁵⁴ ICCPR GEN. COMM. NO. 31, *supra* note 39 at ¶11.

⁵⁵ *See*, ICCPR GEN. COMM. NO. 29, *supra* note 43.

⁵⁶ IHL Database - Introduction to Fundamental Guarantees, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_intofugu (last visited Jul 2, 2022); *see also* UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, INTERNATIONAL LEGAL PROTECTION OF HUMAN RIGHTS IN CONFLICT, HR/PUB/11/01, 55–58 (2011), https://www.ohchr.org/sites/default/files/Documents/Publications/HR_in_armed_conflict.pdf

⁵⁷ STEVEN R. RATNER, JASON ABRAMS & JAMES BISCHOFF, ACCOUNTABILITY FOR HUMAN RIGHTS ATROCITIES IN INTERNATIONAL LAW: BEYOND THE NUREMBERG LEGACY 12 (3rd ed. 2009); *see also* Legal Framework - International Law Applicable to Situations of Armed Conflict, RULAC GENEVA ACADEMY (2017), <https://www.rulac.org/legal-framework>.

and the problem to be addressed, be it the rule emanating from IHL or from International Human Rights Law.⁵⁸

The Human Rights Committee of the United Nations, which oversees implementation of the ICCPR, has similarly observed that “[d]uring armed conflict, whether international or non-international, rules of international humanitarian law become applicable and help [...] to prevent the abuse of a State’s emergency powers.”⁵⁹ Lest there be any doubt, the Committee understands by this that “the Covenant applies also in situations of armed conflict to which the rules of international humanitarian law are applicable.”⁶⁰ It further affirms that generally speaking, while “more specific rules of international humanitarian law may be specially relevant for the purposes of the interpretation of Covenant rights, both spheres of law are complementary, not mutually exclusive.”⁶¹ Moreover, where emergency measures under ICCPR Article 4 are invoked, “no [such] measure derogating from the provisions of the Covenant may be inconsistent with the State party’s other obligations under international law, particularly the rules of international humanitarian law.”⁶²

So what does the concurrent and “complementary” application of IHL and IHRL mean *in practice*? The challenge is deciphering *when* as well as *what* rules of decision from one body of law will apply in a particular scenario rather than those of the other, given that both sets of norms are equally in effect. Navigating the nodal question of what rules of IHL will prevail over those of IHRL in the context of armed conflict depends on the outcome of three fact-specific inquiries fixed by international law. The first is whether the armed conflict is of an international or non-international character, because the instruments, norms and dynamics of IHL that will apply to each are different.⁶³ The second question asks whether there has been a legitimate derogation from the relevant human rights treaties in effect.⁶⁴ The third and final inquiry is that of the *lex*

⁵⁸ IHL and Human Rights - 1. Rights Protected by Both Branches: The Lex Specialis, *in* ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR? , <https://casebook.icrc.org/law/ihl-and-human-rights> (last visited Jul 29, 2022); *see also* UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *supra* note 56; *see also* Marko Milanovic, *The Lost Origins of Lex Specialis: Rethinking the Relationship Between Human Rights and International Humanitarian Law*, *in* THEORETICAL BOUNDARIES OF ARMED CONFLICT AND HUMAN RIGHTS 38, 5 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2463957.

⁵⁹ ICCPR GEN. COMM. NO. 29, *supra* note 43 at ¶ 3.

⁶⁰ ICCPR GEN. COMM. NO. 31, *supra* note 39 at ¶11.

⁶¹ *Id.*

⁶² ICCPR GEN. COMM. NO. 29, *supra* note 43 at ¶9; *id.*, at ¶11 (“States parties may in no circumstances invoke article 4 of the Covenant as justification for acting in violation of humanitarian law [...], for instance by taking hostages, by imposing collective punishments, through arbitrary deprivations of liberty or by deviating from fundamental principles of fair trial, including the presumption of innocence.”).

⁶³ E4J University Module Series: Counter-Terrorism - Module 6: Military / Armed Conflict Approaches to Countering Terrorism, UNITED NATIONS OFFICE ON DRUGS AND CRIME (2018), <https://www.unodc.org/e4j/zh/terrorism/module-6/key-issues/categorization-of-armed-conflict.html>.

⁶⁴ Derogations, *in* ICRC CASEBOOK - HOW DOES LAW PROTECT IN WAR , <https://casebook.icrc.org/glossary/derogations> (last visited Jul 6, 2022).

Human rights law applies at all times except where derogations are permitted in a “state of emergency.” For example, the International Court of Justice in its advisory opinion in *Nuclear Weapons* recognized that: “The protection of the [ICCPR] does not cease in times of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency.” *Legality of the Threat of Nuclear Weapons (Nuclear Weapons)*, Advisory Opinion, 1996 ICJ 226, §25 (Jul. 8), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule7.

specialis (the “special” law), meaning which of the applicable legal norms is more precise in context and thus better suited to the particular scenario addressed.⁶⁵ By working through these threshold issues in the context of the Ukrainian armed conflict, we can begin to see how each body of law is utilized in practice.

As a consequence of the international armed conflict triggered by Russia’s invasion in February 2022, Ukraine has lawfully derogated from both the ICCPR and the ECHR.⁶⁶ I highlighted already the significance of derogation: it is the process through which States may legitimately suspend a number of their legal obligations under the respective treaty, thus drastically reducing its scope of protection to a handful of pre-defined “non-derogable” rights.⁶⁷ In the case of Ukraine’s derogation under ICCPR Article 4 for example, this means that the main treaty protections left in force are the rights to life (Art. 6), juridical personality (Art. 16), and to freedom of thought, conscience and religion (Art. 18); together with the prohibitions on torture (Art. 7), slavery (Art. 8), debt bondage (Art. 11), and ex post facto laws (Art. 15).⁶⁸ In addition, international law recognizes that fair trial and other basic due process guarantees must also remain in effect to ensure the safeguarding of the non-derogable rights.⁶⁹

As the UN Human Rights Committee recognized, derogation leaves a normative vacuum of sorts for IHL to fill as per the terms of its more specialized conventional and customary law framework.⁷⁰ For our purposes, then, the upshot of Ukraine’s derogation under ICCPR Article 4 is that it can enact substantial restrictions on freedom of expression and privacy rights in its territory, even onerous ones, so long as said restrictions conform to the exigencies of the (dire) situation and are not patently arbitrary or discriminatory.⁷¹ It could conceivably adopt measures that would otherwise violate the dictates of ICCPR Art. 20, such as disseminating propaganda for war so long as they did not contravene an applicable principle or rule of IHL.⁷² But what of those core human rights protections that remain in effect in Ukraine even after derogation? What happens in situations of armed conflict where the State cannot or chooses not to derogate from its human rights obligations? These are the scenarios in which the concurrent application of IHL and IHRL will require an inquiry into the *lex specialis*. In Parts II and III below we will explore further how to conduct such an inquiry.

⁶⁵ *Lex Specialis*, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, <https://casebook.icrc.org/glossary/lex-specialis> (last visited Jul 6, 2022).

⁶⁶ *See supra* note 44.

⁶⁷ *See Id.* and accompanying text.

⁶⁸ ICCPR, *supra* note 36, at Arts. 4, 6, 7, 8, 11, 15, 16, 18.

⁶⁹ *Id.* at Art. 4(1).

See also, ICCPR GEN. COMM. NO. 29, *supra* note 43 at ¶¶ 8, 13, 15, and 16.

(“As certain elements of the right to a fair trial are explicitly guaranteed under international humanitarian law during armed conflict, the Committee finds no justification for derogation from these guarantees during other emergency situations.”).

⁷⁰ ICCPR GEN. COMM. NO. 29, *supra* note 43, at ¶9.

⁷¹ *Id.* at ¶16 (“Safeguards related to derogation [...] are based on the principles of legality and the rule of law inherent in the Covenant as a whole.”);

Id. at ¶8 (“According to article 4, paragraph 1, one of the conditions for the justifiability of any derogation from the covenant is that the measures taken do not involve discrimination solely on the ground of race, colour, sex, language, religion or social origin.”).

⁷² *See*, discussion *infra* at notes 148-166 and accompanying text.; *see also*, ICCPR GEN. COMM. NO. 29, *supra* note 43, at ¶3.

For now, an example suffices. An illustration of how *lex specialis* works in the Ukrainian context is provided by Article 15 of the European Convention on Human Rights, which prescribes that treaty's derogation regime. Paragraph 1 of Article 15 affirms that in "time of war or other public emergency threatening the life of the nation" any State party can derogate from its obligations under the Convention. A notable exception is made in Paragraph 2, which states that there can be "[n]o derogation from [the right to life], *except in respect of deaths resulting from lawful acts of war* (emphasis added)."⁷³ (The only other express exceptions made are for the prohibitions on torture, slavery and ex post facto laws.⁷⁴) The ECHR in this way both recognizes the primacy of IHL with respect to the (otherwise non-derogable) right to life in a time of war, and incorporates it as the *lex specialis*. This approach similarly holds true for obligations under other IHRL treaties such as the ICCPR, as recognized by the International Court of Justice.⁷⁵ The ICJ in *Nuclear Weapons* analyzed the interplay between IHL and IHRL with respect to the non-derogable human right not to be arbitrarily deprived of life.⁷⁶ It concluded that "the test of what is an arbitrary deprivation of life [...] falls to be determined by the applicable *lex specialis*, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities."⁷⁷

II. PART TWO

Understanding when and how IHRL and IHL apply to situations of armed conflict is not the end of our analysis but rather the beginning. It is the starting point for the exploration of "real-world" scenarios in which ICT companies confront competing government demands from belligerents and non-belligerents alike. The international law regime described in Part I permits us to discern which set of rules will govern a State's conduct in varying conditions, providing the appropriate normative reference-markers for companies facing such demands. It confirms that international armed conflict *can* under certain circumstances justify a belligerent government's censorship and data requests on its own territory where hostilities are taking place, even if those demands would otherwise be inconsistent with applicable human rights law. This is especially true where a State like Ukraine has derogated lawfully from its human rights obligations in a time of war. Under those circumstances, the "conflict" between IHL and IHRL becomes largely non-existent or minimal in practice.⁷⁸ In that scenario, as in Ukraine today, it is IHL which is presumed to predominate in most cases.

But the question begged here is this: Should tech companies be engaging in the analysis of IHL at all? Is not reliance on the more familiar models already developed pursuant to the UN General Principles on Business and Human Rights sufficient to do the job adequately? The disorientation of ICT company executives and Business and Human Rights ("BHR") officers facing government demands in the face of international armed conflict is understandable.⁷⁹ But the fact remains that even under the UNGP model itself, they, like the governments they

⁷³ ECHR, *supra* note 36, at Art. 15(2).

⁷⁴ *Id.* at Arts. 3, 4, 7(1).

⁷⁵ IHL Database - Introduction to Fundamental Guarantees, *supra* note 56.

⁷⁶ *Id.*

⁷⁷ *Nuclear Weapons*, *supra* note 64, at §926.

⁷⁸ *See infra* Part III.

⁷⁹ Bernard and Nikolova, *supra* note 18 at 892.

interface with, are subject to a different set of relevant international law norms than just human rights when operating in and around theaters of war, namely, IHL.⁸⁰ Whether in Ukraine, Russia or anywhere else in the world where armed conflict exists, the basic tenet of the UNGP model is that companies are expected to respect and promote “international standards” relating to human rights in their interactions with governments.⁸¹ Given the affinity in principles and purpose that inheres within these two overlapping bodies of law,⁸² the UNGP’s operating premise holds equally true where the relevant standards emanate from IHL as when they come from IHRL. This in turn requires developing new analytical pathways to determine what the applicable standards are in the context of armed conflict, especially international armed conflict.⁸³

Fortunately, as Part I shows, such pathways do exist; they require only deliberate development from within the general UNGP framework already in place and adaptation to the challenges faced by tech companies specifically.⁸⁴ Otherwise, ICT companies would be unable to fulfill their duty fixed by that framework to hold governments to their international obligations when making demands or enacting laws and regulations impacting digital rights, and to “seek ways to honor the principles of internationally recognized human rights to the greatest extent possible.”⁸⁵ As a rule, business executives from any sector dealing with potential or actual armed conflict will assess “whether [they] have people at risk, operations that might be affected, or supply chains that might be interrupted[.]” as well as any exposure to cyber-attacks.⁸⁶ To that list of due diligence to-dos, executives must now add the responsibility to ensure they do not make decisions that enable, aid and abet, or otherwise establish complicity in the commission of war crimes and other violations of international law by belligerents.⁸⁷ ICT companies are no exception; in fact, given their nodal role in the digital age, such companies are increasingly being held “accountable not only to their users but to society at large.”⁸⁸

To help discern the pathways possible in this respect, the remainder of Part II is divided into two Sections. In the first, I build on the foundation laid in Part I to analyze the “real-world” examples referenced in the Introduction of government demands arising in the context of the Ukraine conflict.⁸⁹ In Section One, I discuss the appropriate perspectives for analyzing Russian government conduct with respect to that conflict and then contrast those with related actions taken by the European Union. In Section Two, I step back to examine the broader international legal framework upon which the aforementioned events are taking place and how it shapes

⁸⁰ See UNGP, *supra* note 15.

⁸¹ See Global Network Initiative, *supra* note 19, at 2; UNGP, *supra* note 15.

⁸² See *supra* note 18 and accompanying text; see also *infra* note 166 and accompanying text.

⁸³ Interview with Jennifer Easterday, JustPeace Labs, June 14, 2022.

⁸⁴ See *infra* Part III(2).

⁸⁵ Global Network Initiative, *supra* note 19, at 2.

⁸⁶ Paul R. Kolbe, Maria Robson Morrow & Lauren Zabierek, *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*, HARVARD BUSINESS REVIEW: CYBERSECURITY AND DIGITAL PRIVACY (2022), <https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict>.

⁸⁷ See *supra* note 18 and accompanying text; see e.g., UN Guiding Principles, *supra* note 14, at 19–20; Ethical Principles Guiding the ICRC’s Partnerships with the Private Sector, INTERNATIONAL COMMITTEE OF THE RED CROSS, March 10, 2018, <https://www.icrc.org/en/document/ethical-principles-guiding-icrc-partnerships-private-sector>.

⁸⁸ Irene Khan, UN Special Rapporteur on Freedom of Expression and Opinion, *Disinformation and freedom of opinion and expression*, A/HRC/47/25 (13 April 2021), para. 95.

⁸⁹ See *supra*, Part I Introductory discussion, notes 1, 18-19 and accompanying text (Russian, Ukraine and EU examples).

analysis of the Ukrainian-Russian conflict in particular. To do so I focus on recent developments in international legal process as applied to the ICT sector and international security generally. The main goal of Part II is to set the stage for a more in-depth study in Part III of how the two bodies of international law – IHRL and especially IHL – interact in the context of international armed conflict, and how tech companies can adapt their business and human rights assessment models to incorporate it.

A. The Russian-Ukrainian Armed Conflict

In the first Part, I discussed in some detail the situation of Ukraine regarding the operation of IHL and IHRL in that country. Let us now examine in similar fashion the nature and extent of Russia’s obligations after its invasion of Ukraine in early 2022. Significantly, the corresponding panorama of legal obligations for Russia is quite different from that of Ukraine’s outlined above, a fact which has important repercussions for the analysis of government and ICT company responses to Russian propaganda, disinformation and cyber operations in the region.

To begin, we must differentiate between Russian territory proper, and that which it controls or disputes (through conquest) in Ukraine. Let us focus first on the latter. For the most part, the conduct of hostilities following the invasion has been confined to the territory of Ukraine; most of the fighting is currently concentrated in disputed areas along the Russian border to the east and south, especially in the Donbas region, which at the time of this writing was close to being fully occupied.⁹⁰ It is evident that Russia must adhere to the laws of war in the context of these hostilities, as well as in relation to protected persons, such as POWs, wherever they are, i.e. in Ukraine *or* Russia. In particular, Russia is bound to comply with the dictates of Geneva Convention IV, Protocol I and the customary IHL norms applicable to occupied territories in those areas of Ukrainian territory under its control.⁹¹ This is true regardless of whether it respects its obligations or flaunts them, as when Russian forces deliberately commits war crimes to advance their strategic objectives.⁹² The question of whether Russia’s IHRL duties outlined below extend to the occupied zones, to supplement the baseline IHL guarantees for protected

⁹⁰ The Visual Journalism Team, *Ukraine War in Maps: Tracking the Russian Invasion*, BBC NEWS, July 4, 2022, <https://www.bbc.com/news/world-europe-60506682>.

⁹¹ See Natia Kalandarishvili-Mueller, *Russia’s “Occupation by Proxy” of Eastern Ukraine - Implications Under the Geneva Conventions*, (2022), <https://www.justsecurity.org/80314/russias-occupation-by-proxy-of-eastern-ukraine-implications-under-the-geneva-conventions/>. ([following discussion of effective control vs. overall control standards, and grave breaches regime as they apply to occupied territory by government or proxy forces] – “Russia has to fully abide by the international humanitarian law of military occupation in this particular situation. More specifically, Geneva Convention IV should be applicable to the actions of the Russian backed separatists, along with other rules of international humanitarian law. All are also bound by the application of human rights law, applicable to all the warring parties.”); see also, What Happened on Day 74 of the War in Ukraine, NEW YORK TIMES, May 8, 2022, <https://www.nytimes.com/live/2022/05/08/world/ukraine-russia-war-news?smid=url-copy#russia-tightens-its-control-over-occupied-ukraine>.

⁹² See Ukraine: Apparent War Crimes in Russia-Controlled Areas - Summary Executions, Other Grave Abuses by Russian Forces, HUMAN RIGHTS WATCH, April 3, 2022, <https://www.hrw.org/news/2022/04/03/ukraine-apparent-war-crimes-russia-controlled-areas>; Russian War Crimes in Ukraine: EU Supports the International Criminal Court Investigation with €7.25 Million, COUNCIL OF EUROPE, PRESS RELEASE, June 8, 2022, https://ec.europa.eu/commission/presscorner/detail/en/IP_22_3543; One Killing Among Many in a Kyiv Suburb: The Story of a Summary Execution in Bucha, THE ECONOMIST, April 5, 2022, <https://www.economist.com/europe/2022/04/05/one-killing-among-many-in-a-kyiv-suburb>.

persons there, is an open one in theory.⁹³ In practice, however, it seems quixotic at best, for reasons explained further below.⁹⁴

A very different scenario plays out in Russia proper at least insofar as the applicable normative framework is concerned. Given the general absence of hostilities in that country to date, Russia is bound first and foremost to respect human rights law fully *vis-à-vis* all persons within its territory, unless it were to derogate from the operable IHRL treaties.⁹⁵ For example, even if Russia were to seek it (which does not appear to be the case), a valid derogation under the ICCPR is unlikely given the present lack of an apparent existential threat to the nation.⁹⁶ This is especially important in light of the astonishing fact that Russia was expelled from the Council of Europe in March 2022, and as a result will cease to be an active State party to the European Convention on Human Rights starting in September 2022.⁹⁷ That fact notwithstanding, Russia would nonetheless remain bound by IHRL obligations at home and in any place it controls, such as occupied territories in Ukraine, when IHL does not otherwise operate as *lex specialis*.⁹⁸ Even after it ceases to be subject to the dictates of the ECHR, Russia will still be subject to the full panoply of protections prescribed by the ICCPR until such time as it lawfully derogates from them or withdraws from the treaty.⁹⁹

It is for this reason that in May 2022 the United Nations Special Rapporteur on freedom of opinion and expression and her colleagues from other regional human rights systems issued a Joint Statement collectively condemning (in diplomatic terms) Russia's censorship and disinformation campaigns at home in conventional human rights terms.¹⁰⁰ In their statement, these international experts expressed their deepening alarm at

[...] the [...] tightening of censorship and repression of dissent and pluralist sources of information and opinion in the Russian Federation, including the blocking of social media platforms and news websites, [and] disruption of services from foreign content and service providers [...]. *We call on the Russian government to fully implement its international human rights obligations, including by respecting, promoting and protecting the freedom to seek, receive and impart information regardless of frontiers,*

⁹³ See *supra* note 58 and accompanying text. See also *infra* notes 201 – 203 and accompanying text.

⁹⁴ See *infra* note 103 and accompanying text.

⁹⁵ See *supra*, note 64 and accompanying text.

⁹⁶ See ICCPR GEN. COMM. NO. 29, *supra* note 43 at ¶3.

⁹⁷ Kanstantsin Dzehtsiarou & Laurence Helfer, *Russia and the European Human Rights System: Doing the Right Thing... but for the Right Legal Reason?*, EJIL: TALK! (2022), [https://www.ejiltalk.org/russia-and-the-european-human-rights-system-doing-the-right-thing-but-for-the-right-legal-reason/#:~:text=On%2016%20March%202022%2C%20the,on%20Human%20Rights%20\(ECHR\).](https://www.ejiltalk.org/russia-and-the-european-human-rights-system-doing-the-right-thing-but-for-the-right-legal-reason/#:~:text=On%2016%20March%202022%2C%20the,on%20Human%20Rights%20(ECHR).)

⁹⁸ See *supra* notes 90-94 and accompanying text.; see also, ICCPR GEN. COMM. NO. 31, *supra* note 39 at ¶3.

⁹⁹ Even if Russia were to withdraw from the ICCPR, it would still be bound by customary international law and basic human rights protections it recognizes. See, GENERAL COMMENT NO. 26: CONTINUITY OF OBLIGATIONS, CCPR/C/21/REV.1/ADD.8/REV.1 ¶1 (1997), <https://digitalibrary.un.org/record/249474?ln=en> (“Consequently, the possibility of termination, denunciation or withdrawal must be considered in light of applicable rules of customary international law which are reflected in the Vienna Convention on the Law of Treaties.”).

¹⁰⁰ Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER OF HUMAN RIGHTS, May 4, 2022, <https://www.ohchr.org/en/statements-and-speeches/2022/05/ukraine-joint-statement-russias-invasion-and-importance-freedom>.

and by ensuring a safe working environment for independent media, journalists and civil society actors [emphasis added].¹⁰¹

It is worth noting that, in their pronouncement, these experts reference those incidents, raised in the Introduction, of Russia pressuring tech companies to censor social media posts and other information inside the country on platforms like Facebook, YouTube and Twitter.¹⁰² At the same time, they are similarly denouncing as unlawful under IHRL the related measures that were already in place restricting domestic access to those same sites and others, for undermining freedom of expression in Russian territory.¹⁰³

Having mapped the situation under international law prevailing with respect to the *belligerent* States, Russia and Ukraine, only one question remains: What legal parameters apply to *non-belligerent countries* that take actions motivated by the armed conflict between the two countries, like those adopted by the European Union? In March 2022, in a precursor action to the enactment of the Digital Service Act's "crisis mechanism,"¹⁰⁴ the Council of the European Union unanimously passed Regulation 2022/350 banning the transmission over any media of content from two Russian television stations with strong links to the Kremlin.¹⁰⁵ The European Council's resolution denounces Russia's invasion of Ukraine together with the country's "concerted [pro-war] propaganda actions targeted at civil society in the [European] Union [which] constitute a significant and direct threat to the Union's public order and security."¹⁰⁶ The EU describes the two Russian media outlets as "essential and instrumental" to disseminating Russian state propaganda and disinformation directed at EU countries in support of its "illegal military actions" in Ukraine.¹⁰⁷

The EU's stated legal basis for censoring the two Russian media outlets is anchored *inter alia* in the common foreign and security policy rules of the EU.¹⁰⁸ What is interesting for our purposes, however, is the express verdict of all 27 EU member states that the enactment of Regulation 2022/350 – an unprecedented, momentous and sweeping action to be sure – harmonizes with their individual and collective human rights obligations:

In view of the gravity of the situation, and in response to Russia's actions destabilising the situation in Ukraine, it is necessary, *consistent with the fundamental rights and freedoms recognised in the Charter of Fundamental Rights, in particular with the right to freedom of expression and information as recognised in Article 11 thereof*, to introduce

¹⁰¹ *Id.*

¹⁰² See Milmo, *supra* note 8. And accompanying text.

¹⁰³ Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, *supra* note 99.

¹⁰⁴ Meaker, *supra* note 2.

¹⁰⁵ COUNCIL REG. (EU) 2022/350 OF 1 MAR. 2022 AMENDING REG. (EU) NO 833/2014 CONCERNING RESTRICTIVE MEASURES OF RUSSIA'S ACTIONS DESTABILISING THE SITUATION IN UKRAINE, REG. (EU) 2022/350 (2022), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2022.065.01.0001.01.ENG.

¹⁰⁶ *Id.* at ¶7.

¹⁰⁷ *Id.* at ¶9.

¹⁰⁸ Lomas, *supra* note 4.

[these] restrictive measures to urgently suspend the broadcasting activities of such media outlets in the [European] Union, or directed at the Union [emphasis added].¹⁰⁹

What these EU governments are saying – including those of human-rights champions like Estonia, Finland, Netherlands and Sweden – is that they believe the restrictive measures imposed by the Regulation meet “the three-part test of legality, legitimate aim, and necessity and proportionality” required by international human rights law, as reflected in ICCPR article 19(3).¹¹⁰ With respect to the critical third prong of this test – that the restrictions must be in proportion to the problem addressed – the EU officials stress that they are targeting only the two most prominent and clearly attributable outlets used by the Russian state to wage its widespread disinformation campaigns, and only for the duration of the Ukraine conflict.¹¹¹ Indeed, the organic connection between the TV stations targeted and Kremlin is well-documented, bolstering the validity of the EU’s action.¹¹²

Naturally, not everyone agrees. The UN Special Rapporteur on freedom of expression and her regional colleagues, in their joint statement of May 2022, expressed concern that “the EU’s decision to ban two Russian state-owned media outlets may have been a disproportionate response to disinformation.”¹¹³ In their view, “[p]romoting access to diverse and verifiable information, including ensuring access to free, independent and pluralistic media, is a more effective response to disinformation.”¹¹⁴ Be that as it may, there seems to be no dispute that the EU’s weighty aim is legitimate under the circumstances, or that legal process was pursued to advance it (though some have taken issue with it).¹¹⁵ As for the sanctions themselves, when contrasted with the Kremlin’s iron-fisted repression and blocking of all independent media inside Russia (and in Russian controlled territories),¹¹⁶ the focused restrictions enacted by the EU in its Regulation seem to pale by comparison, making it harder to argue against them.¹¹⁷ The only thing that is certain is that this debate will continue to take place exclusively within a human rights

¹⁰⁹ REG. (EU) 2022/350, *supra* note 104 at ¶10.

¹¹⁰ Ukraine: Joint Statement on Russia’s Invasion and Importance of Freedom of Expression and Information, *supra* note 99; ICCPR, *supra* note 36, at Art. 19(3).

¹¹¹ Lomas, *supra* note 4.

¹¹² U.S. DEPARTMENT OF STATE - GLOBAL ENGAGEMENT CENTER, *GEC Special Report - Kremlin-funded Media: RT and Sputnik’s Role in Russia’s Disinformation and Propaganda Ecosystem*, (2022), <https://www.state.gov/report-rt-and-sputniks-role-in-russias-disinformation-and-propaganda-ecosystem/>. Update. “Russia’s aggression against Ukraine: EU adopts ‘maintenance and alignment’ package,” *Consilium*, July 21, 2022, <https://www.consilium.europa.eu/en/press/press-releases/2022/07/21/russia-s-aggression-against-ukraine-eu-adopts-maintenance-and-alignment-package/>.

¹¹³ Ukraine: Joint Statement on Russia’s Invasion and Importance of Freedom of Expression and Information, *supra* note 99.

¹¹⁴ *Id.*

¹¹⁵ The author participated in a Chatham House virtual discussion on May 13, 2022, convened by the Annenberg Public Policy Center, of the University of Pennsylvania, entitled “To Bend or Ban: How should Online Platforms and Services Respond to Armed Conflicts?” Several panelists raised concerns about Regulation 2022/350, including questions about the legitimacy of the “legal process.”

¹¹⁶ The Stalinisation of Russia: As it Sinks in that he Cannot Win in Ukraine, Vladimir Putin is Resorting to Repression at Home, *THE ECONOMIST*, March 12, 2022, <https://www.economist.com/leaders/2022/03/12/the-stalinisation-of-russia>.

¹¹⁷ Vivek Krishnamurthy, *Putin’s Illegal War Has Gotten an Easy Ride from Big Tech*, CENTER FOR INTERNATIONAL GOVERNANCE INNOVATION (2022), <https://www.cigionline.org/articles/putins-illegal-war-has-so-far-gotten-an-easy-ride-from-big-tech/>.

framework, with the armed conflict in Ukraine functioning primarily as context and as a critical source of factual inputs for the analysis of government restraints imposed on freedom of expression under the established “three-part test” in IHRL.¹¹⁸

B. International Law, Cyberspace and Armed Conflict

Up to this point I have centered our discussion on mapping the parameters of IHL and IHRL incumbent upon the main actors in the international armed conflict between Ukraine and Russian, beginning with the belligerents. In Part III below, I will take specific IHL principles and norms and apply them to a series of detailed factual scenarios involving digital rights that have arisen, or might arise, from the war in Ukraine. In this final section of Part II, however, I want to step back and reference the broader legal framework focusing on recent developments in the evolution of international law as applied to cyberspace in the context of international security. This exercise will provide us with a more comprehensive toolkit for the analysis of the issues at hand, as well as help us to better see the normative contours – and limits – of IHL and IHRL in situations of armed conflict. Finally, it will facilitate the next step of isolating the primary principles and rules prescribed by those bodies of law to analyze in Part III their implementation by States and the business actors – tech companies primarily – with whom they interact under the UNGP framework.

To help properly focus the inquiry advanced in this section, I want first to highlight the factual scenarios which are its ultimate target, including the controversial State practices already described.¹¹⁹ In short, what concerns us is the conduct of governments regarding, or in relation to, information and communications technologies (ICTs) used during armed conflicts for purposes *other than as means and methods of warfare*, such as “cyber-attacks.”¹²⁰ For reasons of relevance and practicality, cyber-warfare *per se* has been excluded from our immediate purview.¹²¹ Instead, when we talk about governments’ use of ICTs *other than as means and methods of warfare*, we are talking about actions that include cyber-enabled information operations of “influence,”¹²² such as directed campaigns to spread misinformation and disinformation.¹²³ These operations similarly encompass all types of State propaganda that is disseminated or retransmitted online, which like disinformation, is actively amplified through social media.¹²⁴ Similarly, governments are using digital technologies to enable “unprecedented levels” of surveillance of civilians, with real-world repercussions such as arrest and detention,¹²⁵ at the same time that they may present demands to ICT companies for access to personal and other data further undermining privacy

¹¹⁸ See, e.g., GNI Statement: E.U. Sanctions on Russian Broadcasters (Aug. 2022), available at <https://globalnetworkinitiative.org/eu-sanctions-russia-ukraine-foe/>.

¹¹⁹ See *supra* discussion in Introduction.

¹²⁰ INTERNATIONAL COMMITTEE OF THE RED CROSS, *supra* note 27 at 26–29; see also, *supra* Introduction, discussion on means and methods of war and demarcation; see also, Horowitz, *supra* note 25; see also, MICROSOFT - DIGITAL SECURITY UNIT, *Special Report: Ukraine - An Overview of Russia’s Cyberattack Activity in Ukraine*, (2022), <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd>.

¹²¹ See *supra* Introduction.

¹²² MICROSOFT - DIGITAL SECURITY UNIT, *supra* note 120 at 15.

¹²³ INTERNATIONAL COMMITTEE OF THE RED CROSS, *supra* note 27 at 26–29.

¹²⁴ *Id.*

¹²⁵ *Id.*

rights.¹²⁶ They may even bypass the companies to gain direct access to such data.¹²⁷ Last but not least, as we saw in prior sections, States act or seek to restrict, block or otherwise censor certain online content their government deems offensive or counter to its interests.¹²⁸

Despite increasing State practices of this nature, international law has been slow to recognize, much less address, the threats they pose. To be clear, “IHL does not necessarily prohibit such activities [unless they] adversely affect civilian populations.”¹²⁹ However, it is of great concern to many, and the gravamen of this Article, that the aforementioned types of government conduct, when taken in the context of armed conflict, can leverage “the greater scope and force-multiplying effect provided by digital technology [to] exacerbate – and add to – the existing vulnerabilities of persons affected by armed conflicts.”¹³⁰ For this reason, the United Nations’ entity charged with studying “how international law applies to the use of information and communications technologies by States,”¹³¹ established in 2004, finally recognized in 2021 that “international humanitarian law [...] applies to cyber-operations during an armed conflict[.]”¹³² Although this landmark acknowledgment comes heavily qualified,¹³³ and speaks mostly to governments’ conduct of hostilities in and through cyberspace, it nonetheless portends a normative shift towards recognizing that traditional IHL protections for civilians and “civilian objects” will extend to the actions of belligerents taken through, or in relation to, ICTs.¹³⁴ I will say more about how these protections relate to the questions we are exploring further below.

The UN body spearheading these efforts is the “Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security,” or GGE for short.¹³⁵ The GGE’s groundbreaking 2021 report builds on a series of foundational principles it adopted in an earlier report, from 2015;¹³⁶ taken together, these pronouncements now frame the discussion of how IHL (and IHRL) should be construed in any cyber-related setting to which they apply.¹³⁷ The first of the 2015 principles, reaffirmed by the GGE in 2021, states that “State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within

¹²⁶ See *infra* Part III, B.

¹²⁷ See, Global Network Initiative, *Defining Direct Access*, <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd> (last visited Jul 6, 2022).

¹²⁸ See, e.g., Satariano, *supra* note 9; Milmo, *supra* note 8.

¹²⁹ INTERNATIONAL COMMITTEE OF THE RED CROSS, *supra* note 27, at 28.

¹³⁰ *Id.*

¹³¹ General Assembly resolution establishing the 2019-2021 GGE, A/RES/73/266 (2018), ¶3, <https://undocs.org/A/RES/73/266>.

¹³² Michael Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace*, JUST SECURITY (2021), <https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/>.

¹³³ *Id.*

¹³⁴ See *Id.*, (Noting the open question of whether “data is an ‘object’” such that an operation that targets civilian data for destruction or deletion violates IHL.)

¹³⁵ *Id.*

¹³⁶ GGE 2019-2021 REPORT, *Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security 2019-2021*, ¶¶2-3 (2021), <https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf>; GGE 2015 REPORT, *of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, 2–3 (2015), <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement>.

¹³⁷ Schmitt, *supra* note 132.

their territory.”¹³⁸ It acknowledges that “States exercise jurisdiction over the ICT infrastructure [by] setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats.”¹³⁹ Similarly, the GGE in 2021 reaffirmed its earlier explanation that “[e]xisting obligations under international law are [equally] applicable to States’ ICT-related activity.”¹⁴⁰ The latter principle is especially important to the current study because it recognizes that States’ exercise of their sovereign prerogatives will be bound by legal duties, *inter alia*, to “respect and protect the human rights of individuals over whom they exercise control.”¹⁴¹

The door was thus open for the GGE in 2021 to take the next logical step of affirming what most observers already knew to be true: that IHL plays a similar, limiting role in situations of armed conflict using or involving digital technologies.¹⁴² In 2015, the GGE had gone so far as to acknowledge the operation in cyber-space of “established international legal principles [that apply to the use of ICTs by States], including [...] the principles of humanity, necessity, proportionality, and distinction,”¹⁴³ but stopped short of naming IHL specifically. Its 2021 report not only reiterated these principles, but also integrated them with the GGE’s express recognition of “international humanitarian law” as the context in which those four principles apply, thereby providing “an additional layer of understanding” to guide their further exploration and implementation.¹⁴⁴ Connecting the two concepts in this way moved the normative ball forward significantly.¹⁴⁵ Lest there be any doubt as to what the GGE intended, it highlighted “the need for further study on how and when these [IHL] principles apply to the use of ICTs by States[.]”¹⁴⁶ Before proceeding in Part III to do just that, it behooves us to first review what each of the aforementioned legal principles means, beginning with the “cornerstone” principle of distinction.¹⁴⁷

The principle of distinction requires parties to an armed conflict to distinguish between combatants and civilians, as well as between military and civilian objects.¹⁴⁸ A cardinal rule of IHL is that civilians must be distinguished from combatants, for the simple reason that “[o]ne must know how and what may be targeted and who and what may not, and what protection to afford depending on the category which a person belongs to.”¹⁴⁹ Civilians by definition are non-combatants, because they do not take a direct part in the hostilities, and must therefore be given the granted the highest level of protection afforded by IHL.¹⁵⁰ Basically this means that they

¹³⁸ GGE 2015 REPORT, *supra* note 136, at ¶ 27; GGE 2019-2021 REPORT, *supra* note 136, at ¶ 71(b).

¹³⁹ GGE 2019-2021 REPORT, *supra* note 136, at ¶ 71(b).

¹⁴⁰ GGE 2015 REPORT, *supra* note 136, at ¶ 28(b); GGE 2019-2021 REPORT, *supra* note 136, at ¶ 71(b).

¹⁴¹ Schmitt, *supra* note 132.

¹⁴² *Id.*

¹⁴³ GGE 2015 REPORT, *supra* note 136, at ¶ 28(d).

¹⁴⁴ *Id.* at ¶ 71(f); *see also* Schmitt, *supra* note 132.

¹⁴⁵ Schmitt, *supra* note 132.

¹⁴⁶ GGE 2019-2021 REPORT, *supra* note 136 at ¶ 71(f); *see also*, Schmitt, *supra* note 132.

¹⁴⁷ Principle of Distinction, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, <https://casebook.icrc.org/law/principle-distinction> (last visited Jul 6, 2022).

¹⁴⁸ Legal Framework - International Humanitarian Law, RULAC GENEVA ACADEMY, <https://www.rulac.org/legal-framework/international-humanitarian-law#collapse3accord> (last visited Jul 6, 2022).

¹⁴⁹ Principle of Distinction, *supra* note 147.

¹⁵⁰ *Id.*

cannot be directly targeted by belligerents in the conduct of hostilities,¹⁵¹ although additional protections under both IHL and IHRL will also apply in certain circumstances such as the military occupation of territories.¹⁵² A parallel set of proscriptions operate with respect to civilian *objects*, which must be distinguished from military *objectives*.¹⁵³ International law is clear: “Attacks may only be directed against military objectives. Attacks must not be directed against civilian objects”.¹⁵⁴ The International Court of Justice, in *Nuclear Weapons*, affirmed that the obligation to distinguish during armed conflict between civilians and combatants, on the one hand, and civilian and military objectives on the other, was a “cardinal” and “intransgressible” principle of IHL.¹⁵⁵

The principles of necessity and proportionality are closely linked in IHL. The principle of necessity “permits measures which are actually necessary to accomplish a legitimate military purpose and are not otherwise prohibited by international humanitarian law.”¹⁵⁶ It further limits the degree and kind of force used in military operations to that required to pressure the enemy into a partial or complete submission as soon as feasible, “with minimum expenditure of life and resources.”¹⁵⁷ Proportionality, in turn, functions as a limiting factor in otherwise necessary military actions: “The principle of proportionality [...] seeks to limit damage [in] military operations by requiring that the effects of the means and methods of warfare used must not be disproportionate to the military advantage[s] sought.”¹⁵⁸ It thus prohibits attacks against otherwise legitimate military objectives where the impact of the attack in terms of death or injury

¹⁵¹ IHL Database - Customary IHL - Rule 1. The Principle of Distinction between Civilians and Combatants, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 (last visited Jul 10, 2022). State practice establishes this rule as a norm of customary international law applicable in both international and non-international armed conflicts; the principle of distinction is now codified in Articles 48, 51(2) and 52(2) of Additional Protocol I, to which no reservations have been made. *Id.*

¹⁵² See e.g., GENEVA CONVENTION (IV), *supra* note 24 at Arts. 2, 4, 11, §III. (Pertaining to the rights of protected persons in occupied territories.)

¹⁵³ IHL Database - Customary IHL - Rule 7. The Principle of Distinction between Civilian Objects and Military Objectives., INTERNATIONAL COMMITTEE OF THE RED CROSS 7, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule7 (last visited Jul 10, 2022).

¹⁵⁴ *Id.* State practice establishes this rule as a norm of customary international law applicable in both international and non-international armed conflicts. *Id.* This rule is codified in Articles 48 and 52(2) of Additional Protocol I, to which no reservations have been made. *Id.*

¹⁵⁵ *Id.*; see also, NUCLEAR WEAPONS, *supra* note 64, at ¶79.

¹⁵⁶ Military Necessity, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, <https://casebook.icrc.org/glossary/military-necessity#:~:text=The%20E2%80%9Cprinciple%20of%20military%20necessity,prohibited%20by%20international%20humanitarian%20law> (last visited Jul 10, 2022). The principle of proportionality in attack is codified in Article 51(5)(b) of Additional Protocol I, and repeated in Article 57, and is a settled rule of customary international law. Fundamentals of IHL, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/law/fundamentals-ihl#_ftn_075 (last visited Jul 10, 2022).

¹⁵⁷ International Committee of the Red Cross, *What is IHL?*, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS (2015), <https://www.icrc.org/en/document/what-ihl#:~:text=The%20principle%20of%20military%20necessity,expenditure%20of%20life%20and%20resources>.

¹⁵⁸ Proportionality, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, <https://casebook.icrc.org/glossary/proportionality> (last visited Jul 6, 2022).; The principle of proportionality in attack is codified in Article 51(5)(b) of Additional Protocol I, and repeated in Article 57, and is a settled rule of customary international law. IHL Database - Customary IHL - Rule 14. Proportionality in Attack, INTERNATIONAL COMMITTEE OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14 (last visited Jul 10, 2022).

to civilians, and/or damage to civilian objects, is expected to be excessive compared to the military gain sought.¹⁵⁹ The question begged by the foregoing definitions of the necessity and proportionality principles, however, is this: What constitutes a “legitimate military objective?” In short, legitimate military objectives are those that “by their nature, location purpose or use make an effective contribution to military action, and whose partial or total destruction, capture or neutralization [...] offers a definite military advantage.”¹⁶⁰

Last but certainly not least, humanity as a principle is the animating force behind all of IHL.¹⁶¹ Operationally, “the principle of humanity protects those who are not or no longer actively participating in hostilities and provides for their humane treatment at all times.”¹⁶² It further protects combatants and others who “directly participate in hostilities from superfluous injury or unnecessary suffering.”¹⁶³ It does so primarily through codification in the various IHL treaties already referenced, the Geneva Conventions and their Additional Protocols in particular.¹⁶⁴ At the same time, however, this principle functions as a norm of customary international law to ensure that even in situations not covered by these international agreements, “civilians and combatants remain under the protection [...] of international law derived from established custom, from the principles of humanity and [...] the dictates of public conscience.”¹⁶⁵ Not surprisingly, the principles referenced are as much at the core of IHRL as they are of IHL; indeed, the principle of humanity is the common denominator of both: “it is widely recognized nowadays by the international community that [...] human rights obligations derive from the [same] recognition of inherent rights of all human beings [which are] affected both in times of peace and in times of war[.]”¹⁶⁶

Accordingly, we now turn to Part III, where I examine the interplay of IHL and IHRL using specific fact scenarios addressing various digital rights issues that arise in the context of

¹⁵⁹ Proportionality in Attacks (under IHL), WEAPONS LAW ENCYCLOPEDIA, <http://www.weaponslaw.org/glossary/proportionality-in-attacks-ihl> (last visited Jul 6, 2022).

¹⁶⁰ Military Objectives, in ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR? , <https://casebook.icrc.org/glossary/military-objectives> (last visited Jul 6, 2022). The definition of military objectives is codified in Article 52 of Additional Protocol I and is a rule of customary international law).

¹⁶¹ See Jean Pictet, *Development and Principles of International Humanitarian Law*, Martinus Nijhoff and Henry Dunant Institute, Dordrecht/Geneva, 1985, at 66;

see also, Classification - International Armed Conflict, *supra* note 45, (“International humanitarian law rests on a careful balancing between the foundational principles of humanity and military necessity.”)

¹⁶² Legal Framework - International Humanitarian Law, *supra* note 147.

¹⁶³ Superfluous Injury or Unnecessary Suffering, WEAPONS LAW ENCYCLOPEDIA, <http://www.weaponslaw.org/glossary/superfluous-injury-or-unnecessary-suffering> (last visited Jul 6, 2022).

¹⁶⁴ See GENEVA CONVENTION (IV), *supra* note 24 at Arts. 3, 5, 27,37, 40, 100, 127, 158.

¹⁶⁵ Report of the International Law Commission on the work of its forty-sixth session, UN GAOR, 49th Sess., Supp. No. 10, at 317, UN Doc. A/49/10 (1994), https://legal.un.org/ilc/documentation/english/reports/a_49_10.pdf The Martens clause is a principle of customary international humanitarian law that has been largely codified in other IHL instruments; it essentially confirms that the conduct of belligerents remains regulated by customary international law where treaties may not apply. See Rupert Ticehurst, *The Martens Clause and the Laws of Armed Conflict*, 317 INT. REV. RED CROSS (1997), <https://www.icrc.org/en/doc/resources/documents/article/other/57jnhy.htm> (“Until a more complete code of the laws of war has been issued...the inhabitants and the belligerents remain under the protection and the rule of the law of nations, as they result from the usages among civilized peoples, from the laws of humanity and the dictates of public conscience.”)

¹⁶⁶ UN OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS, *supra* note 56, at 5–6.

armed conflict, as well as examine the role of multi-stakeholder initiatives in promoting and facilitating the engagement necessary to better protect those rights within, and beyond, the UNGP framework.

III. PART THREE

The objective of Part III is to examine in more detail how IHRL and IHL function concurrently in the context of international armed conflict to the benefit of protected persons, and how tech companies and their allies can work together to reinforce these protections within the UN Guiding Principles on Business and Human Rights (UNGPR) framework. This final Part is itself divided into two sections. Section One lays out a case study highlighting several digital rights issues that have arisen, or may arise, during armed conflict, using Russia's invasion of Ukraine as the backdrop. This case study has been adapted and expanded from a hypothetical initially developed by Jason Pielemeier, Executive Director of the Global Network Initiative (GNI), as part of its groundbreaking work in this area.¹⁶⁷ I will return to the importance of multi-stakeholder initiatives (MSIs) in general, and of GNI in particular, further below.¹⁶⁸

The issues raised by the Ukraine-based case study force a closer examination of the real-world interplay between IHL and IHRL in the ICT space, which in practice turns out to be much less complementary than the theory of concurrent application suggests. That is the subject of Section Two. After narrating the scenario in its entirety in the first Section, the second one breaks it down into three distinct "segments" in order to pursue separate, though interrelated, analyses. Each segment will encompass a cluster of related issues to facilitate the exercise. All issues explored in Section Two will center on the actions of the belligerents, with an emphasis on State (Russian) conduct when functioning as an occupying power.¹⁶⁹ The ensuing evaluation will draw upon the prior discussions in Parts I and II, *supra*, to build on the exposition therein regarding the applicable bodies of law, their scope of application, and the analyses of select government measures adopted using ICTs to access, curtail or promote certain types of data, content or information.

A. Case Study: Russia's War in Ukraine

Assume that several months after the Russian invasion of Ukraine, Ukrainian mobile network operators (MNOs) in Kyiv receive written demands from Russian military officials to shut down connectivity for the oblast (province) of Donetsk, which they have

¹⁶⁷ See *Aligning Digital Responses to Armed Conflict with Enduring Values*, The GNI Blog, June 16, 2022, <https://medium.com/global-network-initiative-collection/aligning-digital-responses-to-armed-conflict-with-enduring-values-dffb019ae8d> (last accessed Aug. 26, 2022); Arturo J. Carrillo, *Between a Rock and a Hard Place? ICT Companies, Armed Conflict, and International Law*, The GNI Blog, July 1, 2022, <https://medium.com/global-network-initiative-collection/between-a-rock-and-a-hard-place-41f1ac3e62dc> (last accessed Aug. 26, 2022).

¹⁶⁸ See *infra* PART FOUR Final Observations.

¹⁶⁹ The case study assumes that Russia is an occupying power, though there is some debate about whether under international law that is in fact the case at the time of this writing. See Kalandarishvili-Mueller, *supra* note 91 (arguing that occupation "by proxy" is recognized under international law and established in the Donbas/Donetsk region of Ukraine, such that Russia is subject to all the pertinent normative framework prescribed by IHL, including the grave breaches regime, for what occurs there).

captured and occupied, allegedly to protect civilian lives. The MNOs refuse. The Russian military then force Ukrainian MNO employees in the city of Donetsk, first, to shut down all connectivity to the region, and second, to re-route connectivity via Russian networks, install surveillance equipment on local routers, and re-establish consumer connectivity, claiming authority as an occupying force. The MNOs comply. Almost immediately, the Russian military authorities begin monitoring telecommunications in the region and demanding personal data from ISPs and MNOs on the Ukrainian residents remaining in the city of Donetsk, which they justify as necessary security measures.

Once in control of the telecommunications infrastructure for the Donetsk region, the Russian forces permit only authorized news and entertainment sources to be broadcast or distributed throughout the occupied territory. All others are blocked, mirroring the restrictions in effect in Russia itself. The Russian and Ukrainian language television channels and other media outlets broadcasting to the local population in the Donetsk region are filled almost exclusively with reports of Russian military victories and other information promoting Moscow's version of events. At the same time, the Russian authorities use the telecommunications infrastructure they commandeered in Donetsk to transmit and reinforce informational campaigns promoting pro-Russian content throughout the rest of Ukrainian territory. These campaigns appear geared towards shaping public opinion among the civilian population in Ukraine more broadly regarding Russia's valiant efforts to "liberate" the country from "fascism" and foreign influences.

In light of the developments described, the Ukrainian State Service of Special Communications and Information Protection (SSSCIP) based in Kyiv issues two sets of orders. In the first the SSSCIP orders all MNOs still operating in Ukraine to issue text messages to their subscribers in Donetsk explaining that their mobile phone and internet connections are now censored and unsecure, urging them to resist Russian occupation, and encouraging download of VPNs. The SSSCIP invokes its authority under the recent constitutionally enacted law declaring a state of emergency and granting it emergency powers that, among other things, allow it to curtail due process. The MNOs, fearing for employee safety in Donetsk, refuse. Citing cybersecurity concerns, the SSSCIP then orders MNOs to disconnect and disable the cell towers and any transmission of communications services to subscribers in Donetsk. It makes clear that if the MNOs do not implement the order immediately, the Ukrainian authorities are prepared to enforce it directly. The MNOs comply.

The SSSCIP issues a second round of orders to the Ukrainian MNOs in Kyiv aimed at combatting what it denounces as Russian disinformation and war propaganda in the Donetsk region, as well as throughout Ukraine generally. Those orders prohibited MNOs and other ICT operators from broadcasting or enabling, facilitating or otherwise contributing to broadcasting or distributing, any content by media sources, entities or bodies identified by SSSCIP as promoting Russian propaganda or disinformation, including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed. The list of proscribed media sources includes those coming from Russia proper, such as Russia Today in all languages and Sputnik, as well as several

Russian-controlled local stations broadcasting from the Donetsk region. The MNOs comply.

Months later, after protracted fighting, Ukrainian troops and their allies succeed in retaking the Donetsk region from the Russian occupiers who are forced to retreat back into Russian territory. The SSSCIP immediately orders MNOs in Kyiv and Donetsk to dismantle all Russian modifications to the telecommunications networks and re-establish connectivity to subscribers in the region, which they do. However, given continued skirmishes with pro-Russian factions as well as reports of retaliation against locals who collaborated with the occupying forces in Donetsk, the Ukrainian authorities began demanding that the MNOs provide them with real-time location information for certain subscribers under surveillance pursuant to the emergency powers enacted, and without complying with normal due process procedures. The MNOs comply. At the same time, the SSSCIP informs MNOs that it will be installing surveillance equipment similar to that used by the former Russian occupiers to give it direct access to such information and much more, citing the persistent security threats in the region.

B. Analysis of Ukraine Case Study

As noted in the introduction to this Part, I will now break the case study down into three distinct segments, each encompassing a series of related issues to be analyzed. Let us begin with the first and last paragraph comprising Segment 1, which raises basic questions concerning the obligations of belligerents in occupied and formerly occupied territories.

Segment 1:

*Assume that soon after the Russian invasion of Ukraine, Ukrainian mobile network operators (MNOs) in Kyiv receive written demands from Russian military officials to shut down connectivity for the oblast (province) of Donetsk, which they have captured and occupied, allegedly to protect civilian lives. The MNOs **refuse**. The Russian military then order Ukrainian MNO employees in the city of Donetsk, first, to shut down all connectivity to the region, and second, to re-route connectivity via Russian networks, install surveillance equipment on local routers, and re-establish consumer connectivity, claiming authority as an occupying force. The MNOs **comply**. Almost immediately, the Russian military authorities begin monitoring telecommunications in the region and demanding personal data from ISPs and MNOs on the Ukrainian residents remaining in the city of Donetsk, which they justify as necessary security measures.*

(...)

Months later, after protracted fighting, Ukrainian troops and their allies succeed in retaking the Donetsk region from the Russian occupiers who are forced to retreat back into Russian territory. The SSSCIP immediately orders MNOs in Kyiv and Donetsk to dismantle all Russian modifications to the telecommunications networks and re-establish connectivity to subscribers in the region, which they do. However, given continued skirmishes with pro-Russian factions as well as reports of retaliation against locals who

collaborated with the occupying forces in Donetsk, the Ukrainian authorities began demanding that the MNOs provide them with real-time location information for certain subscribers under surveillance pursuant to the emergency powers enacted, and without complying with normal due process procedures. The MNOs comply. At the same time, the SSSCIP informs MNOs that it will be installing surveillance equipment similar to that used by the former Russian occupiers to give it direct access to such information and much more, citing the persistent security threats in the region.

Beginning with the first paragraph, have the MNOs reacted to the Russian demands in line with the applicable international law framework? To respond, we must first outline the well-defined IHL parameters governing a belligerent party's conduct in occupied territories during international armed conflict.¹⁷⁰ A territory is deemed occupied when it falls under the authority and effective control of the adverse foreign armed forces, and such "occupation extends only to the territory where such authority has been established and can be exercised."¹⁷¹ In addition to the basic IHL principles defined in the prior Part – distinction, necessity, proportionality, and humanity – States such as Russia acting as an occupying power are bound by the more detailed rules established in conventional and customary IHL specifically for occupied territories.¹⁷² The duties of the occupying power emanate primarily from the 1907 Hague Convention and its Regulations,¹⁷³ the Fourth Geneva Convention,¹⁷⁴ as well as certain provisions of Additional Protocol I and customary international humanitarian law.¹⁷⁵ It is critical to keep in mind that under this framework, military occupation by definition is treated as a temporary situation and the rights of the occupying power are limited to the period of its duration; the occupying power does not acquire sovereignty over the territory during that time.¹⁷⁶

¹⁷⁰ See International Committee of the Red Cross, *Occupation and Other Forms of Foreign Administration of Territory* (2012), <https://www.icrc.org/en/doc/assets/files/publications/icrc-002-4094.pdf>; see also Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, I.C.J. Rep. 2004 (July 9); Yoram Dinstein, *The International Law of Belligerent Occupation* (Cambridge University Press, 2009).

¹⁷¹ Hague Regulations (No. IV) Respecting the Laws and Customs of War on Land, Art. 42, Jan. 26, 1910, 36 Stat. 2277, T.S. No. 539; International Committee of the Red Cross, *How Does Law Protect in War?* – Glossary: Occupation, <https://casebook.icrc.org/glossary/occupation>; see also Kalandarishvili-Mueller, *supra* note 91 (outlining the various approaches under international law used to determine control over occupied territory by adverse foreign powers during armed conflict); Eyal Benavisti, *The International Law of Occupation* (1st ed. 2006).

¹⁷² See *supra* notes 170 and accompanying text.

¹⁷³ Hague Convention (No. IV) Respecting the Laws and Customs of War on Land, Jan. 26, 1907, 36 Stat. 2277, R.S. No. 539; Hague Regulations (IV), *supra* note 171, at arts. 42-56, International Committee of the Red Cross, Introduction to the Hague Regulations, <https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?documentId=4D47F92DF3966A7EC12563CD002D6788&action=openDocument> ("The provisions of the [...] Hague Conventions of 1899 and 1907, are considered as embodying rules of customary international law. As such they are also binding on States which are not formally parties to them.") (quoting D. Schindler and J. Toman, *The Laws of Armed Conflicts*, Martinus Nijhoff Publisher, 1988, 69-93)

¹⁷⁴ See *supra* note 24 and accompanying text. The relevant provisions are Geneva Convention IV Articles 27-34 and 47-78.

¹⁷⁵ For an exhaustive, if dated, database of customary norms, see the International Committee of the Red Cross, IHL Database, 2005, <https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1>. As noted, for example, the Hague Convention of 1907's rules relating to occupation are binding customary international law. The ICJ has held that "the provisions of the Hague Regulations have become part of customary law...". *Israeli Wall*, *supra* 170, at para. 89.

¹⁷⁶ An occupation is characterized by governing power controlled by the non-local authority. Accordingly, the return of that to local authorities either through annexation by the hostile power, return to the original authority, or transfer

In practice, the occupying power must respect the laws in force in the occupied territory, unless they constitute a threat to its security or an obstacle to the application of the international law of occupation referenced herein.¹⁷⁷ Generally speaking, adverse military forces in occupied territory are bound to “restore law and order and public life” to the extent possible;¹⁷⁸ this means that local laws remain in force except with respect to the occupying power’s security.¹⁷⁹ In this regard, the occupying power may adopt the measures necessary to ensure the security of its forces in the territory.¹⁸⁰ It is worth noting at the same time that “civilians have no obligation towards the occupying power other than the obligation inherent in their civilian status, i.e., not to participate in hostilities.”¹⁸¹ Any persons who take up arms to resist occupation will lose their status as civilians and corresponding protections under IHL.¹⁸² On a related front, “[p]rivate property cannot be confiscated[,]”¹⁸³ except pursuant “local legislation.”¹⁸⁴ Public property and resources can be administered by the occupying power “but only under the rules of usufruct.”¹⁸⁵ Indeed, the occupying power is responsible for exercising public authority and overseeing the territory as did the sovereign State previously controlling the territory, to the extent feasible under the circumstances.¹⁸⁶ As the International Committee of the Red Cross (ICRC) observes,

the obligations of the occupying power can be logically summed up as permitting life in the occupied territory to continue as normally as possible. IHL is therefore strong in protecting the status quo ante, but weak in responding to any new needs experienced by the population in the occupied territory. The longer the occupation lasts, the more shortcomings IHL tends to reveal.¹⁸⁷

of power to some third entity, ends the occupation. See International Committee of the Red Cross, Occupation and international law: questions and answers, §5, Apr. 8, 2004,

<https://www.icrc.org/en/doc/resources/documents/misc/634kfc.htm>

¹⁷⁷ See *id.*

¹⁷⁸ Hague Regulations (IV), *supra* note 171, at Art. 43; *How Does Law Protect in War?*, IV. Special Rules on Occupied Territories. https://casebook.icrc.org/law/civilian-population#iv_8

¹⁷⁹ See Hague Regulations (IV), *supra* note 171, at Art. 43; Geneva Convention (IV), *supra* note 24, at Art. 64; International Committee of the Red Cross, *How Does Law Protect in War?*, *supra* note 178, at IV. Special Rules on Occupied Territories.

¹⁸⁰ *Id.*

¹⁸¹ *How Does Law Protect in War?*, *supra* note 178, at IV. Special Rules on Occupied Territories

¹⁸² IHL provides civilians no right to resist occupation nor liberate occupied territory, except insofar as they might form a *levee en masse* in accordance with Article 4(A)(6) of the Fourth Geneva Convention, *supra* note 24, at art. Article 4(A)(6). Civilians which engage in such acts surrender their protection as civilians for the duration of their direct participation in hostilities. Protocol I, *supra* note 48, Art. 13(3). After their direct participation has ended, such civilians are also liable to prosecution by the occupying power, although they retain their protected status, with the potential exception of their rights to communication. See Geneva Convention (IV), *supra* note 24, at Arts. 4–5; see also *How Does Law Protect in War?*, *supra* note 178, at IV. Special Rules on Occupied Territories.

¹⁸³ *How Does Law Protect in War?*, *supra* note 178, at IV, Special Rules on Occupied Territories; *Occupation and international humanitarian law: questions and answers*, *supra* note 176; Hague Regulations (IV), *supra* note 171, at Art. 46.

¹⁸⁴ *How Does Law Protect in War?*, *supra* note 178, at IV, Special Rules on Occupied Territories; Hague Regulations (IV), *supra* note 171, at Art. 46.

¹⁸⁵ *How Does Law Protect in War?*, *supra* note 178, at IV, Special Rules on Occupied Territories; Hague Regulations (IV), *supra* note 171, at Art. 55.

¹⁸⁶ *How Does Law Protect in War?*, *supra* note 178, at IV, Special Rules on Occupied Territories.

¹⁸⁷ *Id.*

Returning to the first paragraph of the fact pattern, we are told that the mobile network operators based in Kyiv refused written demands from Russian military officials to shut down connectivity for the oblast (province) of Donetsk in order to allegedly protect civilian lives there. Because the Russian occupation in the case study is limited to the Donetsk region, however, the officials issuing such orders did not have the authority to impose their conditions, justified or not, on private ICT actors *outside* that territory who, moreover, were still bound to respect Ukrainian law and authority.¹⁸⁸ Those MNOs were thus well within their rights to refuse those Russian demands.

At the same time, however, the same Russian officials did have the authority to impose certain conditions *within* the occupied territory, that is, with respect to the MNOs based in Donetsk, if (1) the measures enacted were necessary to ensure the security of the Russian forces there, or (2) they were necessary to maintain law and order consistent with local law.¹⁸⁹ It is unlikely that that the first condition demanded of and implemented by the regional MNOs -- re-routing connectivity via Russian networks -- met the criterion of safeguarding the security of the occupying forces because any connection between the two seems tenuous at best. Enabling disinformation and pro-Russian propaganda, as that edict was plainly intended to do, serves different purposes altogether, including the central objective of influencing public opinion.¹⁹⁰ That issue is examined under Segment 3, *infra*.

Whether the second measure -- installing surveillance equipment on local routers to monitor the local population -- was “necessary” to protecting the security of Russian forces, or maintaining law and order, is a fact-specific question dependent on the conditions prevailing in the region at the time it was promulgated.¹⁹¹ But, given the nature of the Ukrainian conflict, it is likely to pass muster in most cases. On the one hand, there is no express right to privacy or data protection in conventional IHL.¹⁹² Efforts to derive safeguards for digital privacy from the general duties owed to civilians as protected persons under the existing IHL framework provide “sparse” protection at best.¹⁹³ On the other, IHL recognizes that the view of what an occupying power might consider “necessary” when adopting security measures “is more permissive than the conception of military necessity” that governs elsewhere under IHL.¹⁹⁴ Given the volatile climate

¹⁸⁸ See *supra* note 215–224 and accompanying text.

¹⁸⁹ See *supra* note 178–179 and accompanying text.

¹⁹⁰ See PART THREE (A).

¹⁹¹ See International Committee of the Red Cross, *Contemporary Challenges to IHL – Occupation: overview*, June 11, 2012, <https://www.icrc.org/en/doc/war-and-law/contemporary-challenges-for-ihl/occupation/overview-occupation.htm> (“... to fulfil those important responsibilities while ensuring its own security, the occupying power is granted important rights and powers, which may also take the form of measures of constraint over the local population when necessity so requires.”).

¹⁹² Omar Yousef Shehabi, *Emerging Technologies, Digital Privacy, and Data Protection in Military Occupation*, in *THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT*, p. 100 (NATO CCDCOE; Russell Buchan and Asaf Lubin eds., 2022), <https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf> (lamenting that “[t]he absence of express rights to privacy and data protection in conventional IHL is unlikely to change anytime soon.”)

¹⁹³ Shehabi, *supra* note 192, at p. 99. For examples of these efforts, see, e.g., Asaf Lubin, *The Rights to Privacy and Data Protection Under International Humanitarian Law and Human Rights Law*, in *RESEARCH HANDBOOK ON HUMAN RIGHTS AND HUMANITARIAN LAW: FURTHER REFLECTIONS AND PERSPECTIVES* 463-492 (Robert Kolb, Gloria Gaggioli and Pavle Kilibarda eds., Edward Elgar, 2022), and Eyal Benavisti, *The International Law of Occupation*, 90; 96-99. (2006).

¹⁹⁴ Shehabi, *supra* note 192, at p. 99.

prevailing in the disputed region of Donetsk, it is likely that surveillance measures enacted under such circumstances would be viewed as necessary under IHL to preserving the occupants' security in the region, and even arguably helping to maintain public order as well.¹⁹⁵ The MNOs were thus justified in complying with Russian demands in this respect (leaving aside for the moment that they probably had no choice and would have been coerced to do so regardless).

Nor does IHRL serve to fill the gaps left by IHL in this scenario, despite its undisputed relevance. It is true that “[IHRL] is widely recognized as applicable in situations of occupation [and] the exploration of the legal interplay between human rights law and occupation law [is] essential, particularly in relation to matters where IHL is silent, vague or unclear (...)”; but it is equally true that this dynamic can apply only to “certain types of activity.”¹⁹⁶ The question for our purposes, therefore, is this: do existing and emerging norms of IHRL apply in the Russian-occupied territory of Ukraine so as to fill the pertinent lacunae left by IHL specifically with respect to the data privacy rights of the civilian population? The answer, I believe, is in the negative, for a variety of reasons. First and foremost, as noted already and discussed in more detail below, “local law” in Ukraine at the time of the events under study encompasses only non-derogable human rights, which do not include privacy (or freedom of expression).¹⁹⁷ Even if we were to assume the concurrent application of IHRL without derogation and IHL, there are still substantive obstacles to attempting to extrapolate data privacy protections from the former body of law to supplement the latter during military occupation. Put simply, the underlying premises that allow for conventional human rights like data privacy to be safeguarded in democratic and rule-of-law settings presumed by IHRL treaties do not hold on the “battlefield,” i.e. in wartime conditions.¹⁹⁸ They are especially “inapposite in the context of military occupation.”¹⁹⁹ This is because, as remarked upon by one expert, “there is something qualitatively different about data in the hands of the occupying power’s armed forces[.] (...) The law of occupation, by its architecture, would thus not seem to admit of (...) a limitation [imposed by data privacy rights]: if intelligence gathering and storage is a legitimate security measure, then any bona fide military necessity would justify its use.”²⁰⁰

¹⁹⁵ Mary Ellen O’Connell has argued that data privacy rights should remain the same in war as in peace. *See generally* Mary Ellen O’Connell, *Data Privacy Rights: the Same in War and Peace*, *The Rights to Privacy*, in *THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT* (NATO CCDCOE; Russell Buchan and Asaf Lubin eds., 2022), <https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf>; at 12. For a number of reasons, many of them outlined throughout this article, I find such arguments unpersuasive.

¹⁹⁶ Occupation and Other Forms of Foreign Administration of Territory, *supra* note 170, at, p. 8.

¹⁹⁷ *See supra* notes 44, 68 – 69 and accompanying text..

¹⁹⁸ *See How Does Law Protect in War?*, *supra* note 178, at Part III. (“While the purpose of both IHL and International Human Rights Law (IHRL) is to obtain respect for the individual, each of these branches of law has its own implementation approaches and specific mechanisms, tailored to the typical situations for which they were created. Violations of IHL typically occur on the battlefield. They can only be addressed by immediate reaction. [IHRL] is more often violated through judicial, administrative or legislative decisions or inaction against which appeal and review procedures are appropriate and meaningful remedies. In the implementation of IHL, the recovery or the improvement of the situation of the victims is central, and therefore a confidential, cooperative and pragmatic approach is often more appropriate. In contrast, the victims of traditional violations of [IHRL] want their rights to be reaffirmed, and therefore seek public condemnation as soon as they spot violations.”)

¹⁹⁹ Shehabi, *supra* note 192, at p. 103.

²⁰⁰ Shehabi, *supra* note 192, p. 105-6.

Another issue concerns the extraterritorial application of a State's human rights duties where it exercises jurisdiction or effective control, such as during occupation in armed conflict. Our prior discussion in Part II, *supra*, established that both the ICCPR and the ECHR are deemed to apply extraterritorially to the actions of State parties in just this way.²⁰¹ This means that in addition to the IHL obligations incumbent upon Russian forces in occupied Donetsk,²⁰² those forces would also be bound to respect the human rights of the civilian population under its control in that region, just as if those civilians resided in Russian territory.²⁰³ Might this be the avenue for filling the IHL lacunae? Probably not. Russia's poor human rights record at home,²⁰⁴ together with its flouting of the laws of war in Ukraine,²⁰⁵ render any discussion of the extraterritorial application of IHRL by Russian forces during its occupation of Ukrainian territory a theoretical one at best (and an absurdity at worst).²⁰⁶ Indeed, in the case study segment under study, the acknowledgement of this possibility brings to the fore a legal paradox: given Ukraine's derogation from its IHRL obligations, the civilians in occupied Donetsk would be entitled to receive greater protection under Russian human rights law applied extraterritorially than they would under IHL or Ukrainian law.²⁰⁷ If nothing else, this paradox demonstrates the practical limits of international law – and human rights -- in times of war. A better response, I submit, is to continue working towards the development of new IHL norms that recognize safeguards for data relating to protected persons and objects in a manner consistent with the unique nature of the laws of war.²⁰⁸

The foregoing helpfully advances the analysis of a related but separate question raised in Segment 1, namely, were the Russian orders intended to maintain public order consistent with “local law”? This is the issue posed in the second paragraph of Segment 1 (the final paragraph of the case study), which describes the provisions promulgated by the Ukrainian authorities after recapturing the occupied territory. Would domestic law have permitted the imposition of the same restrictive measures by Ukrainian forces after recuperating the once occupied territories, and operating under the same or similar circumstances as their predecessors? In addition to dismantling the restrictions imposed by Russian occupiers and reestablishing domestic connectivity, which they are entitled to do,²⁰⁹ the Ukrainians proceeded to impose a number of restraints on telecommunications in the region similar to the ones promulgated by their adversaries. Citing ongoing security concerns and their emergency powers, Ukrainian officials first demanded -- and received -- access to real-time location information for certain subscribers. They also announced they would install surveillance equipment similar to that used by the Russians to give them direct access to such information and more. Assuming the Ukrainian officials go through with these plans, are these actions consistent with their domestic and

²⁰¹ See *supra* note 40–41 and accompanying text.

²⁰² See *supra* note 49, 91–92 and accompanying text.

²⁰³ See *How Does Law Protect in War*, *supra* note 178, at ICJ/Israel, Separation Wall/Security Fence in the Occupied Palestinian Territory, paras. 102 *et seq.*, 111. https://casebook.icrc.org/case-study/icj-israel-separation-wall-security-fence-occupied-palestinian-territory#part_a_para_124.

²⁰⁴ See *supra* note 103 and accompanying text.

²⁰⁵ See *supra* note 92 and accompanying text.

²⁰⁶ See *infra* note 92–94 and accompanying text.

²⁰⁷ See *supra* note 66–69, 92–94 and accompanying text.

²⁰⁸ See *infra* note 247 and accompanying text.

²⁰⁹ See *infra* notes 215–222 and accompanying text (discussing the duties of States under international law with respect to international telecommunications infrastructure)

international legal obligations at the time? Would the MNOs thus be justified in implementing such orders, assuming they had a choice in the matter?

The answer is almost certainly in the affirmative. Recall our discussion in Parts I and II above of the legal frameworks operating in Ukraine, which has derogated from its principal human rights obligations under the ICCPR and the ECHR.²¹⁰ There can be little doubt that the emergency legislation, constitutionally-enacted in response to Russia's invasion of the country, is justified and thus legitimate.²¹¹ That war-time legislation in turn authorizes action under domestic and international law to impose even onerous restrictions on the derogated-from rights to privacy and freedom of expression, which in peace-time would enjoy robust constitutional and legal protections.²¹² As the case study stands, the continued skirmishes with pro-Russian factions and reports of retaliation against local collaborators indicate substantial security challenges that seem to justify strong measures tailored to the volatile conditions of the ongoing armed conflict. So long as such measures are not on their face arbitrary or discriminatory, or implemented in an arbitrary or discriminatory manner, they are presumed to be valid.²¹³ And if such restrictions are most likely valid when adopted by Ukrainian authorities under Ukrainian law to preserve law and order in the war-torn Donetsk region, they are most likely going to be valid under the same "local law" when imposed by Russian forces operating under similar circumstances in the same region.²¹⁴ Although the Donetsk-based MNOs probably did not have much of a choice when confronted by the Russian occupiers' orders to proceed in this way, these orders would appear to fall within international legal parameters.

Segment 2

*In light of the developments described, the Ukrainian State Service of Special Communications and Information Protection (SSSCIP) based in Kyiv issues two sets of orders. In the first the SSSCIP orders all MNOs still operating in Ukraine to issue text messages to their subscribers in Donetsk explaining that their mobile phone and internet connections are now censored and unsecure, urging them to resist Russian occupation, and encouraging download of VPNs. The SSSCIP invokes its authority under the recent constitutionally enacted law declaring a state of emergency and granting it emergency powers that, among other things, allow it to curtail due process. The MNOs, fearing for employee safety in Donetsk, **refuse**. Citing cybersecurity concerns, the SSSCIP then orders MNOs to disconnect and disable the cell towers and any transmission of communications services to subscribers in Donetsk. It makes clear that if the MNOs do not implement the order immediately, the Ukrainian authorities are prepared to enforce it directly. The MNOs **comply**.*

International law today establishes that States as a function of their sovereignty must maintain and safeguard international telecommunications infrastructure on their territory, both

²¹⁰ See *supra* note 44 and accompanying text.

²¹¹ See *id.*

²¹² See *supra* note 42–44 and accompanying text.

²¹³ See *supra* note 42–44 and accompanying text. This means that the three-part test will not apply.

²¹⁴ See *infra* note 197 and accompanying text.

public and private.²¹⁵ Recall that in 2021, the UN Group of Governmental Experts (GGE) affirmed that “international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.”²¹⁶ The GGE explained that “States exercise [such] jurisdiction [by] setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats.”²¹⁷ Moreover, to the extent that such infrastructure is established and/or operated by private companies, the State is equally “obliged to ensure the cyber infrastructure they operate is (...) maintained and safeguarded (...) through the promulgation of domestic laws and regulations.”²¹⁸ The comprehensive nature of this international legal regime insofar as it applies to both public and privately operated cyber telecommunication services is important to understanding its application to the Ukraine-Russia case study.

International law further recognizes that in exercise of its sovereign prerogative, a State “may suspend (...) international cyber communication services within its territory” or block the transmission of any private cyber communication “that appears contrary to its national laws, public order, or (...) that is dangerous to its national security.”²¹⁹ The International Group of Experts that prepared the Tallinn Manual 2.0, in its commentary to these rules, clarified that this authority “encompasses suspension of incoming and outgoing communications, as well as those that transit a State’s territory.”²²⁰ The States’ prerogative in this respect is limited only by “any international law obligations the State concerned may shoulder prohibiting it from doing so in a particular case,” such as IHRL.²²¹ It is important to highlight that these IHL rules are derived from the existing treaty regime established by the International Telecommunications Union (ITU),²²² and are thus anchored in conventional international law. Similarly, the Tallinn 2.0 Group of Experts referenced ITU norms to acknowledge that “where situations arise in which the ability to engage in safety of life or government communications depends on their prioritization, States must give these communications preference.”²²³ In so doing the Experts were concerned more with natural disasters than armed conflict and occupation, though it surely is relevant to the latter scenario as well.²²⁴

The foregoing establishes that a normative regime under IHL is available to guide the analysis of situations like the one described in Segment 2. And to better understand the relevant rules we can refer to State practice. Consider, for example, the Tallinn 2.0 Experts’ view that the Egyptian authorities’ shutdown in 2011 of international internet and mobile telephony in

²¹⁵ Tallinn 2.0, Rule 61 (Michael N. Schmitt ed., 2d ed. 2017) . In contemporary society, the distinction between telecommunications in the domestic realm and international telecommunications is increasingly blurred. *Id. at.* 284-85. For these reasons, among others, we will focus on the latter in this section.

²¹⁶ GGE 2015 REPORT, *supra* note 136 at ¶ 27; GGE 2019-2021 REPORT, *supra* note 136 at ¶ 71(b).

²¹⁷ GGE 2019-2021 REPORT, *supra* note 136 at ¶ 71(b).

²¹⁸ Tallinn 2.0, *supra* note 215, at Rule 61 commentary, paras. 5,7.

²¹⁹ *Id.*, at Rule 62 & commentary, para. 1.

²²⁰ *Id.*, at Rule 62 commentary, para. 3.

²²¹ *Id.*, at Rule 62 commentary, para. 1.

²²² *Id.*, at Rules 61 and 62 commentary.

²²³ *Id.*, at Ch. 11, para 9. It is interesting to note that Tallin 2.0 says nothing about disinformation, which is not surprising given that such cyber operations fall below the cyber-attack threshold. But to the extent they may increasingly give rise to harm to civilians and other protected persons, future editions of the Tallinn Manual will presumably need to address this phenomenon. *See generally* Eian Katz, *Liar’s War*, 914 IRRC 659 (Dec. 2021)..

²²⁴ Tallin, 2.0, *supra* note 215, at Ch. 11, para 9.

response to the civil uprising resulting from the so-called “Arab Spring” was authorized under this framework.²²⁵ If true, turning back to the case study, it is difficult to see how the Ukrainian authorities’ orders to MNOs to issue text messages to subscribers in militarily-occupied Donetsk alerting them to Russian intervention and censorship violated an international norm of those referenced, much less any domestic law (as modified by the state of emergency legislation). In fact, with respect to the former action, the Ukrainian government’s actions may even have been *required* by the State’s duty to “maintain and safeguard” the integrity of the country’s international telecommunications infrastructure.²²⁶ The MNOs’ decision not to comply with this otherwise legitimate set of demands owed more to organizational “first principles” of protecting employees from retaliation and harm, to which it understandably gave priority, than anything else.²²⁷ Likewise, the subsequent order to dismantle and shut down communication services to subscribers in Donetsk for fear of cyberattacks seems amply justified, both by the express IHL norm allowing State suspension or stoppage of cyber communications that threaten national security, as well as by accepted State practice as reflected in the Egyptian example. The MNOs were right to comply in this case with no fear of facilitating or becoming complicit in an international law violation.²²⁸ Even the threats to enforce this order directly if not otherwise complied with by the MNOs would likely fall within the State’s broad prerogatives in the area of cyber-security.²²⁹

A sceptic could challenge this analysis of Segment 2 by pointing out that IHRL might restrict the actions ordered by the Ukrainian government separately from IHL, and thus reconfigure the proper reading of the international telecommunications and humanitarian law norms cited. They would be right to raise the issue. The GGE has stressed, when affirming State prerogatives emanating from sovereignty, that “[e]xisting obligations under international law are [also] applicable to States’ ICT-related activity.”²³⁰ Such obligations include those to “respect and protect the human rights of individuals over whom they exercise control.”²³¹ The Ukrainian State’s power in this respect is thus limited by any IHRL obligations it has “shoulder[ed] prohibiting it from doing so in [a particular] case.”²³² The Tallinn 2.0 Experts recognized this feature of the legal regime when finding that Egypt’s temporary shutdown of telecommunications in 2011 during the Arab Spring complied with the pertinent international obligations; they caveated their conclusion by stating that it was proffered “without prejudice to

²²⁵ *Id.*, at Ch. 11 Rule 62 commentary, para. 4. For context, amid civil unrest and public demonstrations against the government of Hosni Mubarak in Egypt, Egyptian authorities ordered telecommunications companies to cease access to internet, voice, and text messaging for five days. Deji Olukotun and Peter Micek, Esq., *Five years later: the internet shutdown that rocked Egypt*, AccessNow, Jan. 21, 2016, <https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/>.

²²⁶ See *supra* note 218 and accompanying text.

²²⁷ See *supra* note 86 and accompanying text. In transnational business settings involving conflict like this one, international law provides only one normative input into the calculus of ethical and responsible behavior under the UNGP framework; but it is neither the only one in many cases, nor the dispositive one in some.

²²⁸ See *supra* note 86 and accompanying text.

²²⁹ See *supra* notes 215–224 and accompanying text.

²³⁰ GGE 2015 REPORT, *supra* note 136 at ¶28(b); GGE 2019-2021 REPORT, *supra* note 136 at ¶71(b).

²³¹ Schmitt, *supra* note 132.

²³² Tallinn 2.0, *supra* note 215, Rule 62 commentary, para. 1.

the question of whether Egypt's action[s] complied with (...) respect for the international human right to freedom of expression,"²³³ which they almost certainly did not.²³⁴

The point is that we must examine the extent to which the dictates of IHRL may have prohibited any of the otherwise authorized Ukrainian State actions under review from Segment 2. The short answer again is that Ukraine's state of emergency legislation derogating from its IHRL obligations signifies that no such limits were in effect at the time of the events in question.²³⁵ A more interesting query, however, is what outcome follows from a similar scenario where no derogation has taken place? Though speculative, I would venture to say that even if the full panoply of IHRL rights were assumed to be in effect in Ukrainian territory for this scenario, it is not evident that it would lead to different or better outcomes than the IHL principles outlined above. This is especially true given the features of the international armed conflict reflected in the case study, together with the appropriate operation of *lex specialis*.²³⁶

The first set of orders regarding the issuance of government warnings do not on their face seem to impinge on fundamental rights at all, but rather appear directed at preserving them in manner consistent with the State's duty to protect its population under both IHL and IHRL.²³⁷ In this vein, as we have seen, urgent government communications to protect national security and public order must be given priority in times of war as well as peace.²³⁸ Only with respect to the second set of orders would freedom of expression be reasonably implicated, as concerns the Ukrainian authorities' efforts to sever communication links with the occupied territory in the face of serious threats of Russian cyber-attacks. Nevertheless, in that case as well, war-time national security concerns, along with other prevailing exigencies, could justify an exception to freedom of expression under the applicable human rights regime pursuant to the standard "three-part" test, even an exception as categorical as a partial stoppage of cyber communications to the occupied territory.²³⁹ An alternative approach with a similar outcome is provided by the operation

²³³ *Id.*, at Ch. 11 Rule 62 commentary, para. 4.

²³⁴ See, e.g., Wolfgang Benedek and Matthias C. Kettemen, *Freedom of Expression and the Internet* (Council of Europe Publishing 2013) §6.2.1 ("Using the well-established three-part test, already the legality requirement is not met, as the shutdowns [in Egypt in 2013] were not based on law but rather on executive decisions... Complete Internet shutdowns will hardly ever meet the necessity test.")

²³⁵ See *supra* notes 44, 66–69 and accompanying text.

²³⁶ See prior discussion of *lex specialis* and the concurrent application of IHL and IHRL *supra* at notes 73–77 and accompanying text. Much has been written about the proper interpretation and application of *lex specialis* in this context. See e.g. Marko Milanovic, *The Lost Origins of Lex Specialis: Rethinking the Relationship between Human Rights and International Humanitarian Law*, in *Theoretical Boundaries of Armed Conflict and Human Rights* (Jens David Ohlin ed., Cambridge University Press, Forthcoming); OHCHR, *The International Legal Protection of Human rights in Armed Conflict* (2012), at.54-70, available at <https://www.ohchr.org/en/publications/special-issue-publications/international-legal-protection-human-rights-armed-conflict>.

²³⁷ For example, both the ICCPR and ECHR mandate that a state respect and ensure respect for human rights obligations. See ICCPR, *supra* note 36, at Art. 2; ECHR, *supra* note 36, at Art. 1. Similarly, although there is no similar provision to protect one's own civilians, the IHL mandates respect for the civilians of an adversary or neutral party. See Geneva Convention (IV), *supra* note 24, at Art. 4 (protecting those who "find themselves ... in the hands of a Party to the conflict ... of which they are not nationals.)

²³⁸ See *supra* notes 223–224 and accompanying text.

²³⁹ See *supra* notes 36 and accompanying text. See also Benedek and Kettemen, *supra* note 234, at §6.2.1 ("This is not to say, however, that a partial blackout must always be illegal... If the authorities are technologically unable to shutdown the network services that fuel the conflict, and an appropriate law has been democratically passed, it might

of *lex specialis*, which would require the direct application of the specific IHL norm authorizing such cyber stoppages under these circumstances, much in the same way that *lex specialis* underpins IHL's recognition that the killing of combatants during armed conflict does not violate the right to life.²⁴⁰ A fuller discussion of this regime and its import for the case study is set out in response to Segment 3.

Segment 3:

Once in control of the telecommunications infrastructure for the Donetsk region, the Russian forces permit only authorized news and entertainment sources to be broadcast or distributed throughout the occupied territory. All others are blocked, mirroring the restrictions in effect in Russia itself. The Russian and Ukrainian language television channels and other media outlets broadcasting to the local population in the Donetsk region are filled almost exclusively with reports of Russian military victories and other information promoting Moscow's version of events. At the same time, the Russian authorities use the telecommunications infrastructure they commandeered in Donetsk to transmit and reinforce informational campaigns promoting pro-Russian content throughout the rest of Ukrainian territory. These campaigns appear geared towards shaping public opinion among the civilian population in Ukraine more broadly regarding Russia's valiant efforts to "liberate" the country from "fascism" and foreign influences.

(...)

*The SSSCIP issues a (...) round of orders to the Ukrainian MNOs in Kyiv aimed at combatting what it denounces as Russian disinformation and war propaganda in the Donetsk region, as well as throughout Ukraine generally. Those orders prohibited MNOs and other ICT operators from broadcasting or enabling, facilitating or otherwise contributing to broadcasting or distributing, any content by media sources, entities or bodies identified by SSSCIP as promoting Russian propaganda or disinformation, including through transmission or distribution by any means such as cable, satellite, IP-TV, internet service providers, internet video-sharing platforms or applications, whether new or pre-installed. The list of proscribed media sources includes those coming from Russia proper, such as Russia Today in all languages and Sputnik, as well as several Russian-controlled local stations broadcasting from the Donetsk region. The MNOs **comply**.*

This segment highlights a number of contemporary legal challenges relating to the propagation of war propaganda and disinformation, which are increasingly recognized as harmful to civilians in armed conflict settings.²⁴¹ Strictly speaking, neither is prohibited by the

be proportionate, in order to safeguard the lives of others, to introduce brief regional Internet shutdowns as an *ultima ratio*.”)

²⁴⁰ See *supra* notes 73–74 and accompanying text.

²⁴¹ For a general discussion on the nature of modern disinformation, see Jason Pielemeier, *Disentangling Disinformation: What Makes Regulating Disinformation So Difficult?*, 2020 Utah L. Rev. 917, , <https://dc.law.utah.edu/ulr/vol2020/iss4/1/>. For a thorough analysis of disinformation in the context of armed conflict. See Eian Katz, *supra* note 223.;

laws of armed conflict.²⁴² To the contrary: informational deception to advance military objectives through the use of ruses, decoy actions and misinformation is a time-honored tactic in the conduct of hostilities.²⁴³ Such deception is curtailed by IHL only if it rises to the level of “perfidy” or the misuse of protected symbols such as “white flags” or medical insignias to obtain military advantage.²⁴⁴ Indeed, these traditional IHL rules are widely seen as outmoded given modern advances in ICTs and the cyber operations they enable.²⁴⁵ For this reason, a growing number of commentators are clamoring for greater and more specific regulation of information operations in war time.²⁴⁶ Though still under development, a growing international consensus posits that:

[t]he conduct of information operations or activities in armed conflict is subject to the applicable rules of international humanitarian law (...). These rules include, but are not limited to, the duty to respect and ensure respect for international humanitarian law, which entails a prohibition against encouraging violations of IHL; the duties to respect and to protect specific actors or objects, including medical personnel and facilities and humanitarian personnel and consignments; and other rules on the protection of persons who do not or no longer participate in hostilities, such as civilians and prisoners of war.²⁴⁷

Regarding the issues raised in Segment 3, it is evident that existing rules of IHL prohibit neither the Russian occupiers’ deployment of propaganda and disinformation in and from Donetsk, nor the Ukrainian authorities orders directed at combatting the adversaries information operations. As we discovered in the analysis of Segment 2, occupying forces enjoy significant leeway in the interpretation of their authority to take actions to ensure the security of their presence in the region and maintain public order.²⁴⁸ Taking control of telecommunications in the occupied territory might well be justified as an exercise of that authority within the broad limits permitted under contentious circumstances.²⁴⁹ Russian propaganda and misinformation transmitted from the commandeered telecoms infrastructure are calibrated to influence if not “control the narrative regarding the conflict”²⁵⁰ within Donetsk, as well as throughout the rest of Ukrainian territory not under occupation. Such information operations targeting public opinion are not prohibited by IHL.²⁵¹ Indeed, on these facts, none of the Russian occupiers’ actions in this respect would transgress even the emerging principles relating to disinformation in wartime on

²⁴² Robin Geiss and Henning Lahmann, *Protecting the Information Space in Times of Armed Conflict*, JustSecurity, March 3, 2021, <https://www.justsecurity.org/75066/protecting-the-information-space-in-times-of-armed-conflict/>; see also Katz, *supra* note 223, at p. 662

²⁴³ https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule57

²⁴⁴ See *supra* note 175, at Rule 57: Ruses of War, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule65#:~:text=The%20use%20of%20unlawful%20deceptions,intent%20to%20betray%20that%20confidence

²⁴⁵ Geiss and Lahmann, *supra* note 242; see also Katz, *supra* note 223..

²⁴⁶ Geiss and Lahmann, *supra* note 242; see also Katz, *supra* note 223.

²⁴⁷ Dapo Akande et al, *Oxford Statement on International Law Protections in Cyberspace: The Regulation of Information Operations and Activities*, JustSecurity, June 2, 2021, <https://www.justsecurity.org/76742/oxford-statement-on-international-law-protections-in-cyberspace-the-regulation-of-information-operations-and-activities/>

²⁴⁸ See *supra* note 171–187 and accompanying text.

²⁴⁹ See *supra* note 191–200 and accompanying text.

²⁵⁰ Katz, *supra* note 223, at 661.

²⁵¹ See *supra* note 242–245 and accompanying text.

inciting violence against protected persons and objects, or otherwise harming the well-being of the civilian population.²⁵² It follows as well that this reasoning applies to the countermeasures adopted by their Ukrainian adversaries to combat the disinformation operations, so long as those measures are not themselves otherwise prohibited by IHL.²⁵³ In other words, the Ukrainian authorities orders to MNOs to censor the Russian media sources participating in those operations would likewise be permitted under the laws of war, and the MNOs justified in complying with them, at least as far as IHL is concerned.

The next question, of course, is whether both sets of actions by the belligerents would be consistent with IHRL to the extent it is deemed applicable. Returning to the case study, we find that Russia's blanket repression of freedom of expression in Donetsk mirrors its brutal repression of free speech at home, which has been categorically criticized for transgressing human rights.²⁵⁴ But, as we have seen, IHRL does not apply fully to the Donetsk region, a war zone.²⁵⁵ Ukraine's lawful derogation from its human rights obligations under the ICCPR and the ECHR means that the occupying forces under local law would most likely not be transgressing any pertinent rules, unless their propaganda or misinformation was directed at enabling genocide, war crimes or other crimes against humanity.²⁵⁶ Under "local" Ukrainian law amended by the state of emergency legislation, derogation operates to leave only a handful of non-derogable rights in effect.²⁵⁷ These, however, do not include freedom of expression or the press, thereby opening the door to informational policies and practices by the belligerents that do not otherwise violate IHL (e.g. perfidy, war crimes) or international criminal law (genocide, CAH).²⁵⁸ The only alternative would be to argue that the Russian occupying forces were bound by certain rules of IHRL applied extraterritorially, an approach rife with practical and strategic challenges.²⁵⁹ But even then, as the analysis of IHRL below indicates, it is far from clear that such claims would result in a different outcome.²⁶⁰

Assuming for arguments sake, however, that IHRL applied fully to the occupied Donetsk region under Ukrainian law, how should observers analyze the interplay of that body of law with the IHL framework governing in that territory? We know that in such situations the two are held to apply concurrently and, ideally, to complement each other.²⁶¹ But what does that actually mean in practice? Would the IHRL obligations incumbent on Russian forces operating in occupied Donetsk (under Ukrainian or Russian law) require them to curtail or cease their disinformation campaigns? What about the censorship imposed by the Ukrainians seeking to counteract the effects of those campaigns? It is worth recalling that the overlap between IHL and IHRL is functionally limited to a reduced number of fundamental rights such as the rights to life, physical

²⁵² See Katz, *supra* note 223, p. 660; 668.

²⁵³ See *supra* note 242–245 and accompanying text.

²⁵⁴ See *supra* note 100–103 and accompanying text.

²⁵⁵ See *supra* note 191–200 and accompanying text.

²⁵⁶ See *supra* notes 44, 66–69, 71 and accompanying text.] See Ratner, *supra* note 57, at [pin cite], and accompanying text; see also Katz, *supra* note 223, and accompanying text [pin cites needed].

²⁵⁷ See *supra* notes 44, 66–69, 71 and accompanying text.

²⁵⁸ See *supra* note 256 and accompanying text.

²⁵⁹ See *supra* notes 206–208 and accompanying text [citing discussion of paradox created by the scenario]

²⁶⁰ See *infra* notes xx and accompanying text.

²⁶¹ See *supra* note 196 and accompanying text.

integrity and personal liberty.²⁶² Accordingly, at some level, contrasting the two in the context of international armed conflict is a bit like comparing apples and oranges: both are undeniably fruit, but there is arguably more difference between them than similarity. While sharing a common denominator of humanity, the two bodies of law present divergent natures and objectives:

In the implementation of IHL, the recovery or the improvement of the situation of the victims is central, and therefore a confidential, cooperative and pragmatic approach is often more appropriate. In contrast, the victims of traditional violations of [IHRL] want their rights to be reaffirmed, and therefore seek public condemnation as soon as they spot violations. A more legalistic and dogmatic approach is therefore necessary in implementing [IHRL]; indeed, such an approach corresponds to the human rights logic, which historically represents a challenge to the “sovereign”, while respect for IHL can be considered as a treatment conceded by the “sovereign”.²⁶³

Whether or not the human right to freedom of expression is one of those core norms that enjoys concurrent application in practice under IHL is, at best, an open question.²⁶⁴ Some commentators have suggested that the rule of *lex specialis* requires resorting to IHRL to fill certain gaps in IHL, for example, to protect press freedoms in occupied territories.²⁶⁵ But IHL already provides express protections to war correspondents and other journalists: the former are treated as members of the armed forces, while the latter are protected persons akin to civilians.²⁶⁶ Similarly, the right of communication is reserved for both POWs and civilians in occupied territories;²⁶⁷ though admittedly bare-bones as a form of expression, the express right of communication in these situations, like the protections for war correspondents and journalists, belies the suggestion, at least with respect to freedom of expression, that there may be any “accidental” gaps in IHL that require supplementing.

In any event, we proceed now to analyze Segment 3 from the perspective of IHRL’s concept of freedom of expression applied in situations of international armed conflict. According to the UN Special Rapporteur on Freedom of Expression, speaking to the problem of disinformation in general under IHRL,

States should not make, sponsor, encourage or disseminate statements that they know or should reasonably know to be false, or authorize Internet shutdowns as a means of combatting disinformation. They should restrain from restricting freedom of expression

²⁶² *Id.* See also *How Does Law Protect in War?*, *supra* note 178, at II. Protected Rights]

²⁶³ *How Does Law Protect in War?*, *supra* note 178, at III. Implementation

²⁶⁴ See *supra* note 58 and accompanying text.

²⁶⁵ See *id.* (suggesting IHRL fills that gap where IHL is silent)

²⁶⁶ Geneva Convention (III) Relative to the Treatment of Prisoners of War, Art. 4, Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135. <https://www.icrc.org/en/doc/resources/documents/interview/protection-journalists-interview-270710.htm#:~:text=Inasmuch%20as%20they%20are%20civilians,Conventions%20and%20Additional%20Protocol%20I> ; War correspondents are entitled to embed in the armed forces and are accorded POW status if captured. *Id.*

²⁶⁷ See *id.*, art. 71; GC IV, art. 107. It is also true that this right to communication is limited by articles in the POW and Civilians Conventions that allow for some censorship, See GC III, art. 76, GCIV, art. 112. But even that curtailment signals a deliberate decision by the drafters of the Geneva Conventions to regulate the communications of protected persons during the armed conflict.

online or offline except in accordance with the requirements of articles 19(3) and 20(2) of the [ICCPR], strictly and narrowly construed.²⁶⁸

ICCPR Article 19(3) sets out the “three-part” test for permissible State restrictions on freedom of expression, recognizing only those measures that are enacted pursuant to law to advance a legitimate State aim, and that are both necessary and proportional.²⁶⁹ Article 20(2), in turn, requires States to outlaw any and all “advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.”²⁷⁰ It becomes rapidly apparent when contrasting them that, due to the divergent nature and function of each, the IHRL norms cited either conflict or are in tension with the principles, goals and applicable rules of IHL described above.²⁷¹

The clearest example of this is ICCPR Article 20(1), not mentioned by the UN Special Rapporteur, which prohibits any “propaganda for war,” a norm that by definition can only apply in times of peace.²⁷² Indeed, the UN Human Rights Committee in General Comment 11 recognizes this dissonance to an extent when it affirms that “[t]he provisions of article 20, paragraph 1, do not prohibit advocacy of the sovereign right of self-defense (...),”²⁷³ alluding thereby to inherent limits arising in and around international armed conflict. Another example is the use of Internet shutdowns in the national security context, including armed conflict, which under IHL norms applicable to State cyber operations are permitted, if rarely.²⁷⁴ Under extreme circumstances like those arising during a devastating cyber-attack, for example, Internet shutdowns could conceivably even be necessary to protect civilians and essential civilian infrastructure.²⁷⁵ To round out the point, let us return to Segment 3 and the question of whether the Ukrainian authorities orders combatting Russian war propaganda and disinformation emanating from Donetsk (and Russia) were lawful under IHRL (as they were pursuant to IHL).

Differences with IHL notwithstanding, if we assume for the sake of argument that IHRL applies in Ukraine without derogation, we find ourselves facing a situation similar to the one confronted by the EU in its series of resolutions imposing sanctions on select Russian media outlets for similar reasons,²⁷⁶ excepting, of course, the notable fact that Ukraine is actually a belligerent engaged in armed conflict with Russia. The framework outlined in the quote above from the UN Special Rapporteur is the very framework used to analyze the legitimacy of the EU sanctions adopted in response to Russian disinformation, and to find them lacking under human rights law.²⁷⁷ It is also the one that governs in the Segment 3 hypothetical. So, as was the case with the EU’s sanctions, the proposed Ukrainian restrictions would have to be evaluated using

²⁶⁸ UN Special Rapporteur Report, *supra* note 88, para. 88.

²⁶⁹ GENERAL COMMENT NO. 34, Article 19: Freedoms of opinion and expression, CCPR/C/GC/34 ¶ 22 (2011).

²⁷⁰ ICCPR, *supra* note 36, at Art. 20.

²⁷¹ See *supra* note 263 and accompanying text.

²⁷² In addition, there is confusion in modern times as to what constitutes propaganda for war in the digital age, not least because international law provides little guidance. See e.g. GENERAL COMMENT NO. 11, Prohibition of propaganda for war and inciting national, racial or religious hatred (Art. 20), CCPR/C/GC/11 (1983).

²⁷³ See *id.*, at para. 2.

²⁷⁴ See *supra* notes 219–226 and accompanying text.

²⁷⁵ See *supra* notes 223–225 and accompanying text.

²⁷⁶ See *supra* notes 105–112 and accompanying text.

²⁷⁷ See *supra* notes 113–114 and accompanying text.

the “three-part” test established by IHRL for weighing the legitimacy of government measures that seek to limit freedom of expression in furtherance of a legitimate State aim.²⁷⁸ Under this approach, “the armed conflict [functions] primarily as context and a critical source of factual inputs for [the] analysis,”²⁷⁹ meaning that the stresses, contingencies and uncertainties of war must be factored into the analysis of each prong of the “three-part” test.

The incongruence of analyzing wartime sanctions by a belligerent on an adversary’s propaganda and disinformation under a human rights regime configured primarily for peacetime democracies rapidly becomes evident.²⁸⁰ The EU’s sanctions have been criticized, *inter alia*, for failing to meet the necessary and proportional prong of that test, despite the unprecedented nature of the challenge presented by Russia’s documented disinformation campaigns, and the unanimous opinion of all 27 EU countries that their actions are “consistent with the fundamental rights and (...) in particular with the right to freedom of expression and information.”²⁸¹ One cannot help but wonder whether those critics would find the Ukrainian government’s restrictions in Segment 3, which are expressly modeled on the EU’s but even broader, to be equally lacking. The easy answer is that the Ukraine’s status as a belligerent defending itself from invasion and occupation by Russia distinguishes it from the non-belligerent countries that make up the EU, and thus would ultimately tip the scales in its favor. But the question remains: was the proper weight given to the “armed conflict [as] context and a critical source of inputs” into the analysis of the EU’s sanctions under the IHRL “three-part” test for legitimate limits on freedom of expression? The impact of armed conflict in the digital age on non-belligerent States like those that comprise the EU and how to address it are novel and challenging questions that require deeper exploration in academic and policy circles.

What is certain is that, as pointed out already, Ukraine’s lawful derogation under the relevant IHRL treaties ensures that in the circumstances of the case study as originally presented, even onerous censorship measures like these can legitimately be imposed for the duration of the constitutionally enacted state of emergency.²⁸² The foregoing Section, moreover, illustrates the practical and strategic challenges to extrapolating the application of human rights such as those to privacy and freedom of expression, which were configured principally for peacetime and for enforcement through the operation of the rule-of-law, into the context of international armed conflict. Indeed, in my opinion, the perceived “lacunae” in IHL with respect to privacy and freedom of expression are likely no oversight or coincidence in IHL legislation; nor are they in any way inconsistent with State practice over the centuries, including (so far) into modern times.²⁸³ Data privacy in wartime is, relatively speaking, a nascent field,²⁸⁴ while misinformation

²⁷⁸ See UNSR Report, *supra* note 88, at ¶¶ 30–40.

²⁷⁹ Carrillo, *supra* note 167.

²⁸⁰ See e.g. Shehabi, *supra* note 192, at 102–103 (IHRL approaches to data privacy “rests on a theory of *procedural democracy* which is inapposite in the context of military occupation”) (emphasis in original).

²⁸¹ See *supra* note 109 and accompanying text; see also Carrillo, *supra* note 167.

²⁸² See *supra* notes 44, 66–69 and accompanying text.

²⁸³ See Katz, *supra* note 241, at 931–932; see also Shehabi, *supra* note 192, at 96–100.

²⁸⁴ See Buchan and Lubin, Introduction, in THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT, *supra* note 192, 3 (“Looking beyond treaty law, ‘there is practically no international legal jurisprudence, commentaries, or academic literature’ that applies digital rights like the rights to privacy and data protection in times of armed conflict.”)

and propaganda have always been as much a part of war as killing.²⁸⁵ For these reason, I submit, we are bound to accept the dictates of IHL in Segment 3 despite the fact that IHRL arguably would provide the more specific and protective norm, at least until such time that context-specific prohibitions under IHL can be legislated or developed by States.²⁸⁶ On this view, the Ukrainian authorities orders to MNOs to censor the Russian media sources participating in those operations would be permitted to do so under international law, *full stop*.

IV. CONCLUDING OBSERVATIONS

Recall the overarching inquiries highlighted in the Introduction: What is an ICT company to do when operating in the midst of international armed conflict like the one raging in Ukraine? How should tech company executives respond to urgent government demands – often conflicting -- to propagate or censor online content arising in the context of war, including disinformation? And what of their demands to access the personal data or communications of users, ostensibly to safeguard security but nonetheless presenting the potential for abuse? Governments make difficult demands of ICT companies by seeking to impose heavy restrictions on the free flow of information and data privacy via the latter’s digital and social media platforms and mobile networks. This obligates the companies to devise new practices and policies to respond to those demands and the exigent circumstances that create them. To assist in that process, this Article has mapped the contours of the framework under international law that exists to guide company executives – as well as other stakeholders -- seeking to navigate a principled pathway to addressing such challenges. Specifically, I have demarcated the respective scopes of application of IHRL and IHL, as well as clarified the normative interplay between those two bodies of law using real and hypothetical examples drawn from the international armed conflict between Ukraine and Russia.

The war in Ukraine is but the latest in a series of ongoing or recent international armed conflicts that includes hostilities in Afghanistan, Syria, Iraq, India, Ethiopia and Myanmar.²⁸⁷ Unfortunately, it is unlikely to be the last. By delving into the IHL-IHRL nexus and its function in the context of international armed conflict, my aim has been to facilitate the constructive consideration of international legal norms by private sector actors and other non-governmental stakeholders invested in propagating the principle of humanity in this most difficult of settings. Academic (and other) study of the function of digital rights during armed conflict is only just beginning, so many practical issues remain. In particular, there is a need “to discuss and develop [further] guidance for risk assessment, due diligence, and impact assessment in the ICT space.”²⁸⁸ In this regard, I echo the sentiments of the UN Special Rapporteur on Freedom of Expression that progress in confronting these outstanding issues will require “the proactive engagement of

²⁸⁵ See *supra* notes 241–245 and accompanying text.

²⁸⁶ See *e.g.* Katz, *supra* note 241, and accompanying text (noting that IHL must evolve to address disinformation in times of war) ; see also Shehabi, *supra* note 192 and accompanying text (noting similar conclusion regarding privacy rights); but see Mary Ellen O’Connell, Data Privacy Rights, *supra* note 195, at 28.

²⁸⁷ Council on Foreign Relations, Global Conflict Tracker, at <https://www.cfr.org/global-conflict-tracker> (last visited Aug. 28th, 2022).

²⁸⁸ Global Network Initiative, Submission to the Special Rapporteur Report on Freedom of Expression in times of Armed Conflict and other Disturbances, p. 6, <https://globalnetworkinitiative.org/wp-content/uploads/2022/07/GNI-FoE-Conflict-Submission-12July22-1-2.pdf>

States, companies, international organizations, civil society and the media. The need for multi-stakeholder dialogue and partnerships cannot be overstated.²⁸⁹

²⁸⁹ UN Special Rapporteur Report, *supra* note 88, para. 87.