ARTICLE

# BETWEEN A ROCK AND A HARD PLACE?* ICT COMPANIES, ARMED CONFLICT, AND INTERNATIONAL LAW

*Arturo J. Carrillo***

ABSTRACT ..... 59
I. INTRODUCTION ..... 60
II. INTERNATIONAL LAW ..... 67
A. The Operation of International Law ..... 68
B. The Application of International Law ..... 73
III. ARMED CONFLICT ..... 78
A. The Russian-Ukrainian Armed Conflict ..... 81
B. International Law, Cyberspace and Armed Conflict 87
IV. ICT COMPANIES ..... 95
A. Case Study: Russia's War in Ukraine ..... 96
B. Analysis of Ukraine Case Study ..... 98
V. CONCLUSION ..... 123

*ABSTRACT*

*What is an information, communication and technology ("ICT") company to do when operating in the midst of an 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 requests 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*

*maps the contours of the frameworks under international law—international humanitarian and human rights law, primarily—that exist to guide company executives and other stakeholders who seek to follow a principled pathway to addressing such challenges. To that end, the Article first demarcates the respective scopes of application for international humanitarian and human rights law; it then analyzes the normative interplay between those two bodies of law using real and hypothetical examples drawn from the international armed conflict between Ukraine and Russia. By delving into the IHL-IHRL nexus and its function in the context of international armed conflict, the Article facilitates 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.*

## *I. 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

* I would like to thank the following persons for their input on previous drafts of this Article: Jason Pielemeier, Jennifer Easterday, Evelyn Aswad, and Jonathan Horowitz. 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.

** Arturo J. Carrillo is Clinical Professor of Law and founding Director of the Civil and Human Rights Law Clinic at the George Washington University Law School, where he also co-directs the Global Internet Freedom Project.

1. *See* Adam Satariano & Sheera Frenkel, *Ukraine War Tests the Power of Tech Giants*, N.Y. TIMES (Feb. 28, 2022), https://www.nytimes.com/2022/02/28/technology/ukraine-russia-social-media.html?referringSource=articleShare [https://perma.cc/45QS-G9UH].

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 twenty-seven national governments comprising the European Union may invoke the mechanism to censor content they deem a threat arising from the Ukraine conflict, such as war propaganda or disinformation, something the European Union had already acted to do.[4] The European Union's new expanded authority 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 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 technology 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] The Putin government has also ordered platforms outside of Russia to lift their restrictions on pro-Kremlin media outlets related to Ukraine.[9] The Zelenskiy

2. Morgan Meaker, *Ukraine War Prompts Europe's New Emergency Rules for the Internet*, WIRED (Apr. 25, 2022), https://www.wired.com/story/europe-digital-services-act/ [https://perma.cc/6ZGR-8JK8].

3. *Id.*

4. *See* Natasha Lomas, *EU's Ban on Russia Today and Sputnik is Now in Effect*, TECH CRUNCH (Mar. 2, 2022), [https://perma.cc/9S9W-HAFT].

5. *See* Meaker, *supra* note 2.

6. *See id.*

7. *See id.*, Satariano & Frenkel, *supra* note 1.

8. *See* Dan Milmo, *Russia Blocks Access to Facebook and Twitter*, THE GUARDIAN (Mar. 4, 2022), https://www.theguardian.com/world/2022/mar/04/russia-completely-blocks-access-to-facebook-and-twitter [https://perma.cc/D4AC-TCRH].

9. Adam Satariano, *Russia Intensifies Censorship Campaign, Pressuring Tech Giants*, N.Y. Times (Feb. 26, 2022), https://www.nytimes.com/2022/02/26/technology/russia-censorship-tech.html [https://perma.cc/U82V-9ML3].

government in turn sent a letter to Internet Corporation for Assigned Names and Numbers ("ICANN") to urge the non-governmental group to revoke the most common Russian internet domains and shut down the domain name system ("DNS")[10] root 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 is an ICT company to do? How should responsible technology companies respond to government demands to regulate online content arising in and around international armed conflicts, such as war propaganda? 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 technology companies simply required to "choose a side" when presented with competing demands by State parties to the conflict? What about others who are not active belligerents themselves but have expressly sided with one? Or is there a more principled approach to digital realm decision-making in the context of an 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

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 How Does DNS Work?, THOUSAND EYES, PART OF CISCO, https://www.thousandeyes.com/learning/techtorials/dns-domain-name-system [https://perma.cc/NKE4-LGQ8] (last visited July 29, 2022).

11. *See* Jon Brodkin, *Ukraine Asks ICANN to Revoke Russian Domains and Shut Down DNS Root Servers*, ARS TECHNICA (Mar. 2, 2022), https://arstechnica.com/tech-policy/2022/03/ukraine-wants-russia-cut-off-from-core-internet-systems-experts-say-its-a-bad-idea/[https://perma.cc/9XTK-EV8E].

12. *Words and Wars: Ukraine Facing Ukraine Propaganda,* UKR. WORLD (Sept. 7, 2022), https://ukraineworld.org/articles/infowars/words-and-wars-ukraine-facing-russian-propaganda [https://perma.cc/C69B-BHK7].

13. Satariano & Frenkel, *supra* note 1.

to guide their actions during 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 [15] ("UNGP") have been adapted to the business models of ICT companies and applied to the protection of freedom of expression and privacy rights online through 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:

> [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

14. *See UN Guiding Principles*, BUSINESS & HUMAN RIGHTS RESOURCE CENTRE, https://www.business-humanrights.org/en/big-issues/un-guiding-principles-on-business-human-rights/ [https://perma.cc/S4GJ-9NX5].

15. *Guiding Principles on Bus. & Hum. Rts.*, U.N. OFF. OF THE HIGH COMM'R OF HUM. RTS. (2011) https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf [https://perma.cc/P3PA-92JZ].

16. *Protecting and Advancing Freedom of Expression and Privacy in the ICT Sector*, GLOB. NETWORK INITIATIVE, https://globalnetworkinitiative.org/ [https://perma.cc/ED48-DSY2] (last visited Jul 6, 2022); UN Human Rights Office of the High Commissioner, The UN Guiding Principles in the Age of Technology, https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/introduction-ungp-age-technology.pdf [https://perma.cc/5ABZ-4KTV] [hereinafter UNGP].

17. *See* IHL and Human Rights, INTERNATIONAL COMMITTEE OF THE RED CROSS, War and Law https://www.icrc.org/en/war-and-law [https://perma.cc/N8J4-KYUT] (last visited July 6, 2022); IHL and Human Rights, INTERNATIONAL COMMITTEE OF THE RED CROSS, IHL and Human Rights https://casebook.icrc.org/law/ihl-and-human-rights (last visited Oct. 22, 2022).

> 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 response to the touchstone question of how an ICT company should conduct itself in times of war *vis-à-vis* the actions of belligerent governments. 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 the same obligations when faced with contrary government demands.[19] 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 European Union's enactment of the DSA, the United States announced that it and sixty other State "partners" were assuming a series of political commitments to advance "a positive vision for the Internet in the

18. Vincent Bernard & Mariya Nikolova, *Interview with John G. Ruggie*, 94 INT. REV. RED CROSS 891–902, 892-96 (March 2012), https://international-review.icrc.org/articles/intervie w-john-g-ruggie [https://perma.cc/8TTQ-UMZS].

19. *See* Global Network Initiative, *GNI Principles on Freedom of Expression and Privacy*, GLOB. NETWORK INITIATIVE 2–3, https://globalnetworkinitiative.org/gni-principles/ [https://perma.cc/DP3C-6P4D] (last visited July 8, 2022) ("The duty of governments to respect, protect, promote and fulfill human rights is the foundation of this human rights framework.").

20. *Id.*

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 president, Brad Smith, pointedly raised the armed conflict in Ukraine as one of those 21st century challenges. He highlighted 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 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 during wartime serve to orient the policies and practices of ICT companies when belligerent and non-belligerent governments place their demands? 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 during wartime?

---

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/ [https://perma.cc/937M-9755].

22. *Id.*

23. *Id.*

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/ [https://perma.cc/8JZD-HKAD], *See also infra* notes 214-15 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 [https://perma.cc/HQR9-C4AN]; *see infra* Part II: International Law.

In this Article, I will address these and related questions to provide at least preliminary answers to most of them. It is divided into five Parts. I begin Part II by examining when and how the relevant bodies of international law apply to and during armed conflict between States. This second 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 reference to the situation of Ukraine. In Part III, 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 analyses of "real-world" scenarios arising from the armed conflict in Ukraine to focus first on Russia, and then on the European Union. Part III wraps up with an overview of the broader international law panorama within which all these scenarios are taking place. In Part IV, I take a deeper dive into more detailed factual scenarios involving the protection of digital rights in war zones, before concluding in Part V.

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 laws of armed conflict.[25] Russia's

25. *See* Andy Greenberg, *The WIRED Guide to Cyberwar*, WIRED (Aug. 23, 2019) https://www.wired.com/story/cyberwar-guide/, [https://perma.cc/9BHQ-CRL5]; Jonathan Horowitz, *Cyber Operations under International Humanitarian Law: Perspectives from the ICRC*, 24 AM. SOC'Y INT'L. L., May 19, 2020, https://www.asil.org/insights/volume/24/issue/11/cyber-operations-underinternational-humanitarian-law-perspectives-icrc [https://perma.cc/NSA6-PLGY];

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.

## *II. INTERNATIONAL LAW*

In Ukraine, as 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 evaluate whether said demands comport with the State's legal obligations, 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 on armed conflict between nations. In the Section A of this Part, I examine the operation of State duties under international human rights law

---

*see also* Michael N. Schmitt, *'Attack' as a Term of Art in International Law: The Cyber Operations Context*, *in* PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283-93 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012); Gary Corn, *Cyber National Security: Navigating Gray Zone Challenges In and Through Cyberspace*, *in* COMPLEX BATTLESPACES: THE LAW OF ARMED CONFLICT AND THE DYNAMICS OF MODERN WARFARE (Christopher M. Ford & Winston S. Williams eds., 2018).

26. *See* Tom Burt, *The Hybrid War in Ukraine*, MICROSOFT ON THE ISSUES (Apr. 27, 2022), https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/ [https://perma.cc/LMA8-YW9Y].

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 [https://perma.cc/6CX7-GVUY] (last visited July 6, 2022); *see generally* Mason Clark, *Russian Hybrid Warfare*, INST. OF THE STUDY OF WAR (Sept. 2022), https://www.understandingwar.org/report/russian-hybrid-warfare [https://perma.cc/SVY2-GJDN].

28. *See* discussion *infra* Part III.b.

29. *See* GLOB. NETWORK INITIATIVE, *supra* note 19 and accompanying text.

("IHRL") and IHL, as well as how those legal obligations apply to and in a particular country. In Section B, 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 and to non-belligerent countries, like those which comprise 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 to by States, and customary international law ("CIL"), defined as norms that evidence a general practice among nations accepted as law.[30] 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 obligation 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 duties under IHRL and IHL, or otherwise being complicit in such abuses.[32] The starting place in either case is treaty law: what IHL and IHRL treaties the State in question have ratified and what is their scope of application?

While the Vienna Convention on the Law of Treaties' ("VCLT") rules governing treaty ratification and interpretation will apply

30. *Public International Law: A Beginner's Guide—Sources of Law*, LIBR. OF CONG. RSCH GUIDES, https://guides.loc.gov/public-international-law/sources-of-law [https://perma.cc/EEZ6-NZ9R] (last visited June 6, 2022); *see also Customary International Humanitarian Law*, INT'L COMM. OF THE RED CROSS (Oct. 29, 2010), https://www.icrc.org/en/document/customary-international-humanitarian-law-0 [https://perma.cc/4XQM-EXZZ].

31. Int'l L. Comm'n, Draft Articles on Responsibility of States for Internationally Wrongful Acts, U.N. DOC. A/56/10 art. 2 (2001), https://legal.un.org/ilc/texts/instruments/english/commentaries/9_6_2001.pdf [https://perma.cc/JHQ7-TED7].

32. *See* GLOB. NETWORK INITIATIVE, *supra* note 19 at 2 and accompanying text.

equally across the board to all treaties, the precise scope of application of *specific* treaties will vary depending on their express terms.[33] This principle is critical to understanding how to navigate the overlap of IHL and IHRL in situations of armed conflicts. Broadly speaking, the scope of application of each body of law is defined by two factors: (1)the ground rules of international law that apply to treaties, most notably the edict in VCLT Article 26 where "every treaty in force is binding upon the parties [that have subscribed] to it and must be performed by them in good faith;"[34] and (2) the express terms set out in the treaty itself about the scope of application. As with any legally binding agreement, treaties must define, among other things, the subject matter, geographic, and temporal contours of their application. VCLT Article 31(1) 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]

Take Ukraine as an example. Ukraine is a long-time State Party to the International Covenant on Civil and Political Rights ("ICCPR" or "Covenant") and the European Convention on Human Rights ("ECHR");[36] it is also a member of the Council of Europe ("COE").[37]

---

33. *See generally* 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[https://perma.cc/5DP7-86AR] [hereinafter "VCLT" or "Vienna Convention"].

34. *Id.* at art. 26.

35. *Id.* at 31(1).

36. *See* Int'l Covenant on Civil and Political Rights, Dec. 16, 1966, 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[https://perma.cc/3F8D-F9GH] [hereinafter "ICCPR"]; Eur. Convention for the Protection of Hum. Rts. 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 [https://perma.cc/R3K8-YU8F] [hereinafter "ECHR"]; For a list of ratifications, *see* Depositary Status of Treaties, 4. Int'l Covenant on Civil and Political Rights, United Nations Treaty Collection, https://treaties.un.org/Pages/ViewDetails.aspx?chapter=4&clang=_en&mtdsg_no=IV-4&src=IND [https://perma.cc/6RQP-XRWX](last visited Sep 25, 2022). *See also* Chart of Signatures and Ratifications of Treaty 005, Council of Europe, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=005 [https://perma.cc/KVZ5-MCVH](last visited Sep 25, 2022).

37. Council of Europe: 46 Member States, COUNCIL OF EUR., https://www.coe.int/en/web/portal/46-members-states [https://perma.cc/4BEB-RZ9V] (last visited July 6, 2022).

To simplify the exposition moving forward, I will focus on the ICCPR with the understanding that the discussion of how that treaty operates in relation to Ukraine and other States is representative of those countries' conventional human rights obligations more broadly.

The VCLT is clear when it comes to the geographic scope of treaties in general terms. VCLT 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.[39] The ICCPR Human Rights Committee expounded on what is meant by "subject to its jurisdiction;" it said 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 ICCPR 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 undern international law and do not involve discrimination . . .

38. VCLT, *supra* note 33, at art. 29 (emphasis added).

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 [https://perma.cc/G74J-U44G] ("[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*, Işil Karakaş & 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).

." [42] Article 4 thus operates to narrow the ICCPR's scope of application of human rights protections even further in times of existential threats to the State Party, as demonstrated by Ukraine in the wake of Russia's invasion.[43] We will return to this key point further below 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, they will apply "to all 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. For example, Geneva Convention III covers prisoners of war, and is thus known as the POW Convention, while Geneva Convention I and II address combatants rendered *hors de combat* on land and at

42. *See infra* at note 64 and accompanying text; 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, N.Y. TIMES (Mar. 3, 2022), [https://www.nytimes.com/live/2022/03/03/world/russia-ukraine#catch-up-on-the-latest-news-on-ukraine [https://perma.cc/K94W-C9UY]; see also Hum. Rts. Comm., General Comment No. 29, States of Emergency (Art. 4), U.N. Doc CCPR/C/21/Rev.1/Add.11 ¶ 3 (2001), https://digitallibrary.un.org/record/451555?ln=en [https://perma.cc/ED7V-J595]("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. U.N. Off. of the High Comm'r for Hum. Rts., 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 [https://perma.cc/4SAC-9QFN].

45. *Classification of International Armed Conflict*, RULAC GENEVA ACAD. (2017) https://www.rulac.org/classification/international-armed conflict#:~:text=Common%20Article%202%20to%20the,recognized%20by%20one%20of%20them [https://perma.cc/S6RG-Y6JL] (last updated Aug. 30, 2017).

46. Geneva Convention Relative to the Protection of Civilian Persons in Time of War, *supra* note 24, at art. 2.

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 of 1977 known as Protocol I.[48] Ukraine, like Russia, is a long-standing State Party to the four Geneva Conventions and 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 of armed conflict on a State party's territory. To better understand what that means in practice, look no further than the war in Ukraine, an international armed conflict between countries that are subject to the four Geneva Conventions, Protocol I, and customary international humanitarian law.[50] In other words, IHL applies by its own terms *primarily* 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

47 . See Protected Persons, in HOW DOES LAW PROTECT IN WAR?, https://casebook.icrc.org/glossary/protected-persons (last visited Jul 6, 2022). For a brief explanation of the different Geneva Conventions, see, The Geneva Conventions of 1949 and their Additional Protocols, International Committee of the Red Cross, Jan. 1, 2014 https://www.icrc.org/en/document/geneva-conventions-1949-additional-protocols[https://perma.cc/K346-XJAQ].

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 [https://perma.cc/J57T-DED5].

49. *See Treaties, States Parties, and Commentaries—Ukraine*, INT'L COMM. OF THE RED CROSS,https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=UA [https://perma.cc/U85P-2RWS] (last visited July 8, 2022). (G.C. Accession: Aug. 3 1954, Add. Pro. I Accession: Jan. 25, 1990); *see also Treaties, States Parties, and Commentaries: Russian Federation,* INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreatiesByCountrySelected.xsp?xp_countrySelected=RU [https://perma.cc/SF8X-PC32] (last visited July 8, 2022). (G.C. Accession: Oct. 5, 1954, Add. Pro. I Accession: Sept. 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 Belligerency*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/belligerency [https://perma.cc/5NUP-CBUD](last visited July 6, 2022).

taking place and/or *wherever* the "protected persons," 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 summary, 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.

### *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 when 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

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

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 [https://perma.cc/Q3SL-38S5].

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

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

companies and others seeking to understand what rules pertain to scenarios arising through war.[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 (international criminal law is the third body.) [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, described 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 and the problem to be addressed, be it the rule emanating from IHL or from International Human Rights Law.[58]

---

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.pd [https://perma.cc/HLL7-ZAEX].

57 . *See also International Law Applicable to Situations of Armed Conflict*, RULAC GENEVA ACAD. (2017), https://www.rulac.org/legal-framework [https://perma.cc/6RY2-M7U7](last updated Jan. 13, 2017).

58. *IHL and Human Rights, Rights Protected by Both Branches: The Lex Specialis*, ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/law/ihl-and-human-rights [https://perma.cc/YP9K-WHD9](last visited July 29, 2022); *see also* U.N. OFF. OF THE HIGH COMM'R FOR HUM. RTS., *supra* note 44; *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 HUM. RTS. 38, 5 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2463957 [https://perma.cc/NX52-XM4K].

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 that "the Covenant applies also in situations of armed conflict to which the rules of international humanitarian law are applicable."[60] It further affirmed that 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

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 [https://perma.cc/483M-7YF7]. IHL, codified primarily in the Geneva Conventions and customary law after the Second World War, was primarily

question asks whether there has been a legitimate derogation from the relevant human rights treaties in effect.[64] The third inquiry is that of the *lex 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 under the respective treaty's provisions authorizing State parties to do so. 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.[66] 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 (Article 6), juridical personality (Article

designed to address international armed conflict (conflict between states.) In the decades since, non-international armed conflicts, those involving conflict between "organized non-state armed groups" and a State, have become more common. The law addressing these types of conflict is more limited: Common Article 3, Additional Protocol II, and customary IHL govern NIAC's. When Does IHL Apply?, ICRC BLOG (June 13, 2017), https://blogs.icrc.org/ilot/2017/08/13/when-does-ihl-apply/ [https://perma.cc/J6TJ-ASM9].

64. Derogations, *in* ICRC CASEBOOK—HOW DOES LAW PROTECT IN WAR, https://casebook.icrc.org/glossary/derogations [https://perma.cc/M2GP-ASLT] (last visited July 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*, Advisory Opinion, 1996 ICJ 226, ¶ 25 (July 8), https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule7 [https://perma.cc/9YEB-994C] [hereinafter *Nuclear Weapons*].

65. Lex Specialis, *in* ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/glossary/lex-specialis [https://perma.cc/AST3-NGD4] (last visited July 6, 2022).

66. *See id.* and accompanying text.

16), and to freedom of thought, conscience and religion (Article 18), together with the prohibitions on torture (Article 7), slavery (Article 8), debt bondage (Article 11), and ex post facto laws (Article 15).[67] 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.[68]

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.[69] Here, 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.[70] It could conceivably adopt measures that would otherwise violate the dictates of ICCPR Article 20, such as disseminating war propaganda so long as they did not contravene an applicable IHL principle or rule. 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*.

An illustration of how *lex specialis* works in the Ukrainian context is provided by Article 15 of the European Convention on Human Rights ("ECHR"), which prescribes that treaty's derogation regime. Paragraph 1 of Article 15 affirms that in "time of war or

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

68. *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.").

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

70. *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, color, sex, language, religion or social origin."). *See* discussion *infra* at notes 148-66 and accompanying text.; *see also* ICCPR GEN. COMM. NO. 29, *supra* note 43, ¶3.

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*."[71] The only other express exceptions made are for the prohibitions on torture, slavery and ex post facto laws.[72] 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("ICJ").[73] In its advisory opinion, *The Legality of the Threat of Nuclear Weapons* ("*Nuclear Weapons")*, the ICJ analyzed the interplay between IHL and IHRL with respect to the non-derogable human right to not be arbitrarily deprived of life.[74] 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."[75]

## *III. ARMED CONFLICT*

Understanding when and how IHRL and IHL apply to armed conflict is not the end of our analysis but rather the beginning. It is the starting point for exploring "real-world" scenarios in which ICT companies confront competing government demands from belligerents and non-belligerents alike. The international law regime described in Part II 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 conflicts *can*, under certain circumstances, justify a belligerent government's censorship and data requests in its own territory where hostilities

71. ECHR, *supra* note 36, at art. 15(2) (emphasis added).
72. *Id.* at arts. 3, 4, 7(1).
73. IHL Database—Introduction to Fundamental Guarantees, *supra* note 56.
74. *Id.*
75. *Nuclear Weapons*, *supra* note 64, at § 240.

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 wartime. Under those circumstances, the "conflict" between IHL and IHRL becomes largely non-existent or minimal in practice.[76] In that scenario, as in Ukraine today, the IHL is presumed to predominate in most cases.

But the question begged here is this: should technology 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 during an international armed conflict is understandable.[77] But the fact remains that even under the UNGP model itself, they, like the governments they 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.[78] Whether in Ukraine, Russia, or anywhere else in the world where armed conflict exists, the basic tenet of the UNGP model expects companies to respect and promote "international standards" relating to human rights in their interactions with governments.[79] Given the affinity in principles and purpose that inheres within these two overlapping bodies of law,[80] 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 internationally.[81]

Fortunately, as Part II shows, such pathways do exist; they require only deliberate development from within the general UNGP framework already in place and adaptation to the challenges

76. *See infra* Part IV.

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

78. *See* UNGP, *supra* note 16.

79. *See* GLOB. NETWORK INITIATIVE, *supra* note 19, at 2; UNGP, *supra* note 16.

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

81. Virtual in-person Interview with Jennifer Easterday, JustPeace Labs (June 14, 2022).

faced by technology companies specifically.[82] 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."[83] 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.[84] 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.[85] 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."[86]

To help discern the pathways possible in this respect, the remainder of Part III is divided into two sections, which build on the foundation laid in Part II to analyze the "real-world" examples referenced in the Introduction of government demands arising in the context of the Ukraine conflict.[87] In Section A, I discuss the appropriate perspectives for analyzing Russian government conduct with respect to that conflict and then contrast those with

82. *See infra* Part IV.B.

83. GLOB. NETWORK INITIATIVE, *supra* note 19, at 2.

84. Paul R. Kolbe et al., *The Cybersecurity Risks of an Escalating Russia-Ukraine Conflict*, HARV. BUS. REV.: CYBERSECURITY & DIGITAL PRIVACY (2022), https://hbr.org/2022/02/the-cybersecurity-risks-of-an-escalating-russia-ukraine-conflict [https://perma.cc/TVP7-67JH].

85. Bernard & Nikolova *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, INT'L COMM. OF THE RED CROSS (Mar. 10, 2018), https://www.icrc.org/en/document/ethical-principles-guiding-icrc-partnerships-private-sector [https://perma.cc/26UJ-DDVB].

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

87. *See supra* Part I Introductory discussion; *See also* Satariano & Frenkel *supra* notes 1, 18-19 and accompanying text (Russian, Ukraine, and EU examples).

related actions taken by the European Union. In Section B, I step back to examine the broader international legal framework upon which the aforementioned events are taking place and how it shapes 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 III is to set the stage for a more in-depth study in Part IV of how the two bodies of international law—IHRL and especially IHL—interact in the context of international armed conflict, and how technology companies can adapt their business and human rights assessment models to incorporate it.

### *A. The Russian-Ukrainian Armed Conflict*

In Part II, 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 companies' 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, with most of the fighting 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.[88] 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

88. 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 [https://perma.cc/5FR3-TUA7] (At the time of this writing, Donbas was close to being fully occupied).

the customary IHL norms applicable to occupied territories in those areas of Ukrainian territory under its control.[89] This is true regardless of whether it respects its obligations or flaunts them when Russian forces deliberately commits war crimes to advance their strategic objectives.[90] The question of whether Russia's IHRL duties outlined below extend to the occupied zones, to supplement the baseline IHL guarantees for protected persons there, is an open one in theory.[91] In practice, however, it seems quixotic at best, for reasons later explained.[92]

A very different scenario plays out in Russia proper where 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

89. *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/ [https://perma.cc/UUR7-UVEW]; The 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, N.Y. 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 [https://perma.cc/KM2K-T3XG].

90. *See Ukraine: Apparent War Crimes in Russia-Controlled Areas—Summary Executions, Other Grave Abuses by Russian Forces*, HUMAN RIGHTS WATCH (Apr. 3, 2022), https://www.hrw.org/news/2022/04/03/ukraine-apparent-war-crimes-russia-controlled-areas [https://perma.cc/C8BS-GNZF]; 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 [https://perma.cc/A6WZ-UKDT]; *One Killing Among Many in a Kyiv Suburb: The Story of a Summary Execution in Bucha*, THE ECONOMIST (Apr. 5, 2022), https://www.economist.com/europe/2022/04/05/one-killing-among-many-in-a-kyiv-suburb [https://perma.cc/86WG-EAX5].

91. *See* RULAC GENEVA ACAD., *supra* note 57 and accompanying text; *see also infra* notes 201–03 and accompanying text.

92. *See infra* note 102 and accompanying text.

IHRL treaties.[93] 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.[94] 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.[95] 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*.[96] 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 it lawfully derogates from them or withdraws from the treaty.[97]

Hence, 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 Russia's censorship and disinformation campaigns at home.[98] In their statement, these international experts expressed their deepening alarm at:

---

93. *See supra* note 63 and accompanying text.

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

95. Kanstantsin Dzehtsiarou & Laurence Helfer, *Russia and the European Human Rights System: Doing the Right Thing . . . but for the Right Legal Reason?*, EJIL: TALK! (Mar. 29, 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://perma.cc/8A6U-2V3H].

96. *See supra* notes 89-93 and accompanying text*; see also* ICCPR GEN. COMM. NO. 31, *supra* note 39, at ¶ 3.

97. 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://digitallibrary.un.org/record/249474?ln=en [https://perma.cc/2JYB-VYCV] ("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.").

98. UNITED NATIONS OFFICE OF THE HIGH COMMISSIONER OF HUMAN RIGHTS Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, (May 4, 2022), https://www.ohchr.org/en/statements-and-speeches/2022/05/ukraine-joint-statement-russias-invasion-and-importance-freedom [https://perma.cc/CB65-L9ZV].

> [ . . . ] 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*, and by ensuring a safe working environment for independent media, journalists and civil society actors.[99]

It is worth noting that, in their pronouncement, these experts referenced those incidents, raised in the Introduction, of Russia pressuring technology companies to censor social media posts and other information inside the country on platforms like Facebook, YouTube, and Twitter.[100] 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.[101]

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,"[102] the Council of the European Union unanimously passed Regulation 2022/350 banning the transmission of content from two Russian television stations with strong links to the Kremlin over any

99. *Id* (emphasis added).

100. *See* Milmo, *supra* note 8 and accompanying text.

101. Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, *supra* note 98.

102. Meaker, *supra* note 2.

media.[103] The European Council's resolution denounced Russia's invasion of Ukraine and 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." [104] The European Union described the two Russian media outlets as "essential and instrumental" in disseminating Russian state propaganda and disinformation directed at EU countries to gather support of its "illegal military actions" in Ukraine.[105]

The European Union anchored its stated legal basis for censoring the two Russian media outlets *inter alia* in its common foreign and security policy rules.[106] What is interesting, however, is the express verdict of all twenty-seven EU member States that the enactment of Regulation 2022/350—an unprecedented, momentous and sweeping action to be sure—harmonized 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 [these] restrictive measures to urgently suspend the broadcasting activities of such media outlets in the [European] Union, or directed at the Union.[107]

What these EU governments were saying—including those of human-rights champions like Estonia, Finland, Netherlands, and Sweden—is that they believed the restrictive measures imposed by the Regulation met "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). [108] With

---

103. 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://perma.cc/8NG2-QQCJ].

104. *Id.* at ¶ 7.

105. *Id.* at ¶ 9.

106. Lomas, *supra* note 4.

107. REG. (EU) 2022/350, *supra* note 103 at ¶10 (emphasis added).

108. Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, *supra* note 98; ICCPR, *supra* note 36, at art. 19(3); *see also*

respect to the critical third prong of this test—that the restrictions must be proportionate to the problem addressed—the EU officials stressed that they were 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 Ukrainian conflict.[109] Indeed, the organic connection between the TV stations targeted and Kremlin had been well-documented, bolstering the validity of the European Union's action.[110]

Naturally, not everyone agreed. In their May 2022 joint statement, the UN Special Rapporteur on freedom of expression and her regional colleagues expressed concern that "the [European Union]'s decision to ban two Russian state-owned media outlets may have been a disproportionate response to disinformation."[111] 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."[112] Be that as it may, there seems to be no dispute that the European Union's weighty aim was legitimate under the circumstances, or that legal process was pursued to advance it though some have taken issue with it.[113] As for the sanctions

---

European Court Of Justice, PRESS RELEASE No 132/22: Case T-125/22 RT France v Council (July 27, 2022) https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132en.pdf [https://perma.cc/GUM5-AHTC] (announcing the Court of Justice of the European Union's judgment affirming the lawfulness of the European Union's sanctions).

109. Lomas, *supra* note 4.

110. 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/ [https://perma.cc/Y3W8-HZDR];"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/ [https://perma.cc/9KUB-SVL7].

111. Ukraine: Joint Statement on Russia's Invasion and Importance of Freedom of Expression and Information, *supra* note 98.

112. *Id.*

113. 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,

themselves, when contrasted with the Kremlin's iron-fisted repression and blocking of all independent media inside Russia and its controlled territories,[114] the focused restrictions enacted by the European Union in its Regulation seem to pale by comparison, making it harder to argue against them.[115] The only thing that is certain is that this debate will continue to take place exclusively within a human rights 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.[116]

### *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 Russia, beginning with the belligerents. In Part IV 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 III, however, I want to step back and reference the broader legal framework with a focus on recent developments in the evolution of international law on global security in cyberspace. This exercise will provide a more comprehensive toolkit for the analysis of the issues at hand and to better see the normative contours and limits of IHL and IHRL in armed conflicts. Finally, it will facilitate the next step of isolating the primary principles and rules prescribed by

---

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."

114. The Stalinisation of Russia: As it Sinks in that he Cannot Win in Ukraine, Vladimir Putin is Resorting to Repression at Home, THE ECONOMIST (Mar. 12, 2022), https://www.economist.com/leaders/2022/03/12/the-stalinisation-of-russia [https://perma.cc/ZPR4-MGXR].

115. 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/ [https://perma.cc/UD6W-C554].

116. *See, e.g.,* GNI Statement: E.U. Sanctions on Russian Broadcasters (Aug. 2022), *available at* https://globalnetworkinitiative.org/eu-sanctions-russia-ukraine-foe/ [https://perma.cc/9L6P-U8KD].

those bodies of law to analyze in Part IV their implementation by States and business actors—technology 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. [117] In short, what concerns us is the conduct of governments regarding, or in relation to, ICTs used during armed conflicts for purposes *other than means and methods of warfare*, such as "cyber-attacks." [118] For reasons of relevance and practicality, cyber-warfare *per se* has been excluded from our immediate purview.[119] Instead, we are talking about actions that include cyber-enabled information operations of "influence," [120] such as directed campaigns to spread misinformation and disinformation.[121] These operations similarly encompass all types of State propaganda that is disseminated or retransmitted online, which like disinformation, is actively amplified through social media.[122] Similarly, governments are using digital technologies to enable "unprecedented levels" of surveillance of civilians with real-world repercussions such as arrest and detention.[123] At the same time, they may present demands to ICT companies for access to personal and other data, further undermining privacy rights.[124] They may even bypass the companies to gain direct access to such data.[125] Last but not least, States act or seek to restrict, block or

117. *See supra* discussion in Introduction.

118. 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 [https://perma.cc/EBR8-6TWU].

119. *See supra* Introduction, note 138.

120. MICROSOFT - DIGITAL SECURITY UNIT, *supra* note 118, at 15.

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

122. *Id.*

123. *Id.*

124. *See infra* Part IV.B.

125. *See,* Global Network Initiative, *Defining Direct Access*, https://globalnetworkinitiative.org/defining-direct-access-2/#:~:text=Join%20GNI-

otherwise censor certain online content their government deems offensive or counter to its interests.[126]

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."[127] 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."[128] For this reason, the United Nations' entity charged with studying "how international law applies to the use of information and communications technologies by States,"[129] established in 2004, finally recognized in 2021 that "international humanitarian law [ . . . ] applies to cyber-operations during an armed conflict[.]" [130] Although this landmark acknowledgment comes heavily qualified [131] 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.[132] I will say more about how these protections relate to the questions further below.

The UN body spearheading these efforts is the "Group of Governmental Experts on Advancing Responsible State Behavior in

---

,Defining%20Direct%20Access%3A%20GNI%20calls%20for%20greater%20transparency%20and%20dialogue,to%20voice%20and%20data%20communications [https://perma.cc/YG6H-URRL] (last visited July 6, 2022).

126. *See, e.g.*, Satariano, *supra* note 9; *see also* Milmo, *supra* note 8.

127. INTERNATIONAL COMMITTEE OF THE RED CROSS, *supra* note 27, at 29.

128. *Id.* at 28.

129 . G.A. Res. 73/266, ¶ 3 (Jan. 2, 2019), https://undocs.org/A/RES/73/266 (establishing the 2019-2021 GGE).

130 . 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/ [https://perma.cc/8736-CYDQ].

131. *Id.*

132. *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.).

Cyberspace in the Context of International Security" ("GCE").[133] The GGE's groundbreaking 2021 report built on a series of foundational principles it adopted in an earlier report from 2015; [134] taken together, these pronouncements framed the discussion of how IHL and IHRL should be construed in any cyber-related setting to which they apply. [135] The first of the 2015 principles, reaffirmed by the GGE in 2021, stated 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 their territory." [136] It acknowledged 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." [137] Similarly, the GGE in 2021 reaffirmed its earlier explanation that "[e]xisting obligations under international law are [equally] applicable to States' ICT-related activity."[138] The latter principle is especially important to the current study because it recognizes that States' exercise of their sovereign prerogatives will be bound

133. *Id.*

134. Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, transmitted by Letter dated 28 May 2021 from the Chair of the Group Established Pursuant to Paragraph 3 of General Assembly Resolution 73/266 Addressed to the Secretary-General, ¶¶ 2-3, U.N. Doc. A/76/135 (July 14, 2021), https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf [https://perma.cc/HYX2-SCV8] [hereinafter GGE 2019-2021 Report]; Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Letter dated 26 June 2015 from the Chair of the Group Established Pursuant to Paragraph 4 of General Assembly Resolution 68/243 Addressed to the Secretary-General, ¶¶ 2-3, U.N. Doc. A/70/174 (July 22, 2015), https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement [https://perma.cc/P95Q-SXAJ] [hereinafter GGE 2015 Report].

135. Schmitt, *supra* note 130.

136. GGE 2015 Report, *supra* note 134, at ¶ 27; GGE 2019-2021 Report, *supra* note 135, at ¶ 71(b).

137. GGE 2019-2021 REPORT, *supra* note 134, at ¶ 71(b).

138. GGE 2015 Report, *supra* note 134, at ¶ 28(b); GGE 2019-2021 Report, *supra* note 136, at ¶ 71(b).

by legal duties, *inter alia*, to "respect and protect the human rights of individuals over whom they exercise control."[139]

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.[140] 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,"[141] but stopped short of naming IHL specifically. Its 2021 report, however, 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.[142] Connecting the two concepts in this way moved the normative ball forward significantly.[143] 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[.]"[144] Before proceeding in Part IV 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.[145]

The principle of distinction requires parties to an armed conflict to distinguish between combatants and civilians, as well as between military and civilian objects.[146] A cardinal rule of IHL is that civilians must be distinguished from combatants, for the simple reason that "[o]ne must know who and what may be targeted and who and what may not, and what protection to afford

139. Schmitt, *supra* note 130.

140. *Id.*

141. GGE 2015 REPORT, *supra* note 134, at ¶28(d).

142. *Id.* at ¶71(f); *see also* Schmitt, *supra* note 130.

143. Schmitt, *supra* note 130.

144. GGE 2019-2021 REPORT, *supra* note 134, at ¶ 71(f); *see also,* Schmitt, *supra* note 130.

145. Marco Sassóli, et al., *Principle of Distinction*, *in* HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/law/principle-distinction (2014) (ebook).

146. *International Humanitarian Law*, RULAC GENEVA ACAD., https://www.rulac.org/legal-framework/international-humanitarian-law#collapse3accord [https://perma.cc/R3SH-QVSB] (last visited July 6, 2022).

depending on the category which a person belongs to."[147] 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.[148] They cannot be directly targeted by belligerents in the conduct of hostilities.[149]

Additional protections under both IHL and IHRL will also apply in certain circumstances, such as the military occupation of territories.[150] A parallel set of proscriptions operate with respect to civilian *objects*, which must be distinguished from military *objectives*.[151] International law is clear: "[a]ttacks may only be directed against military objectives. Attacks must not be directed against civilian objects".[152] The International Court of Justice in *Nuclear Weapons* affirmed that the obligation to distinguish during an armed conflict between civilians and combatants, and civilian and military objectives was a "cardinal" and "intransgressible" principle of IHL.[153]

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

147. Sassóli, et al., *supra* note 145.

148. *Id.*

149. IHL Database - Customary IHL, *Rule 1. The Principle of Distinction between Civilians and Combatants*, INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule1 [https://perma.cc/24Q5-RAKC] (last visited July 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.*

150. *See e.g.*, Geneva Convention (IV) Relative to the Treatment of Civilian Persons, arts. 2, 4, 11, § III, Aug. 12, 1949, T. I. A. S. No. 3365, 75 U.N.T.S. 287 [hereinafter Geneva Convention (IV)]. (pertaining to the rights of protected persons in occupied territories).

151. IHL Database Customary IHL, *Rule 7. The Principle of Distinction between Civilian Objects and Military Objectives.,* INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule7 [https://perma.cc/59AU-T7G2] (last visited July 10, 2022).

152. *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.*

153. *Id.*; *see also,* NUCLEAR WEAPONS, *supra* note 64, at ¶¶ 78-79.

and are not otherwise prohibited by international humanitarian law."[154] It further limits the degree and kind of force used in military operations required to pressure the enemy into a partial or complete submission as soon as feasible "with minimum expenditure of life and resources."[155] Proportionality functions as a limiting factor in otherwise necessary military actions: "[it] 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."[156] It thus prohibits attacks against otherwise legitimate military objectives where the impact of the attack in terms of death or injury to civilians and/or damage to civilian objects is expected to be excessive compared to the military gain sought.[157] The question raised by the foregoing definitions of the necessity and proportionality 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

154. Military Necessity, *in* ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, [https://perma.cc/R3K2-ZZ2D](last visited July 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/glossary/military-necessity#:~:text=The%20%E2%80%9Cprinciple%20of%20military%20necessity,prohibited%20by%20international%20humanitarian%20law [https://perma.cc/8AHS-N327] (last visited July 10, 2022).

155. International Committee of the Red Cross, *What is IHL?*, INTERNATIONAL HUMANITARIAN LAW: ANSWERS TO YOUR QUESTIONS (Sept. 18, 2015), https://www.icrc.org/en/document/what-ihl#:~:text=The%20principle%20of%20military%20necessity,expenditure%20of%20life%20and%20resources [https://perma.cc/U3WE-CJAU].

156. *Proportionality*, *in* ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/glossary/proportionality [https://perma.cc/5RRY-7CPK] (last visited July 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. *See IHL Database - Customary IHL - Rule 14. Proportionality in Attack,* INT'L COMM. OF THE RED CROSS, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter4_rule14 [https://perma.cc/643K-JTHR] (last visited July 10, 2022).

157. *Proportionality in Attacks (under IHL)*, WEAPONS LAW ENCYCLOPEDIA, http://www.weaponslaw.org/glossary/proportionality-in-attacks-ihl [https://perma.cc/D83G-QJ77] (last visited July 6, 2022).

destruction, capture or neutralization [. . . ] offers a definite military advantage."[158]

Last but certainly not least, humanity as a principle is the animating force behind all of IHL.[159] 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."[160] It further protects combatants and others who directly participate in hostilities from superfluous injury or unnecessary suffering.[161] It does so primarily through codification in the various IHL treaties already referenced, especially the Geneva Conventions and their Additional Protocols.[162] At the same time, 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."[163]

---

158. *Military Objectives*, *in* ICRC CASEBOOK - HOW DOES THE LAW PROTECT IN WAR?, https://casebook.icrc.org/glossary/military-objectives [https://perma.cc/Y87T-NCSA] (last visited July 6, 2022). The definition of military objectives is codified in Article 52 of Additional Protocol I and is a rule of customary international law); *Id.*

159. *See* JEAN PICTET, DEVELOPMENT AND PRINCIPLES OF INTERNATIONAL HUMANITARIAN LAW 66, (Martinus Nijhoff & Henry Dunant Institute, Dordrecht/Geneva eds., 1985); *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.").

160. Legal Framework - International Humanitarian Law, *supra* note 150.

161. *Superfluous Injury or Unnecessary Suffering*, WEAPONS LAW ENCYCLOPEDIA, http://www.weaponslaw.org/glossary/superfluous-injury-or-unnecessary-suffering [https://perma.cc/K6MS-SENL] (last visited July 6, 2022).

162. *See* GENEVA CONVENTION (IV), *supra* note 150 at arts. 3, 5, 27,37, 40, 100, 127, 158.

163. Report of the International Law Commission on the Work of its Forty-Sixth Session, U.N. GAOR, 49th Sess., Supp. No. 10, at 317, U.N. Doc. A/49/10 (1994), https://legal.un.org/ilc/documentation/english/reports/a_49_10.pdf [https://perma.cc/N782-5VYP]. 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

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."[164] Accordingly, we now turn to Part IV, where I examine the interplay of IHL and IHRL using specific scenarios addressing various digital rights issues that arise in the context of armed conflict within the UNGP framework.

## *IV. ICT COMPANIES*

The objective of Part IV 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 technology companies and their allies can work together to reinforce these protections within the UNGP framework. "This penultimate Part is divided into two sections. Section A lays out a case study highlighting several digital rights issues that have arisen or may arise during armed conflict, such as Russia's invasion of Ukraine. This case study has been adapted and expanded from a hypothetical initially developed by Jason Pielemeier, Executive Director of the Global Network Initiative ("GNI"),[165] as part of its groundbreaking work in this area. [166] I will return to the

[https://perma.cc/UJ29-HBJ6] ("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.").

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

165. Team, Global Network Initiative, https://globalnetworkinitiative.org/team/ [https://perma.cc/N5GS-E5GA] (last visited Sept. 25, 2022).

166. *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 [https://perma.cc/L2BD-DAWC] (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 [https://perma.cc/7ZCC-4BE8] (last accessed Aug. 26, 2022).

importance of multi-stakeholder initiatives ("MSIs") and of GNI further below.[167]

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 B. After narrating the scenario in its entirety, the second one breaks it down into three distinct "segments" to pursue separate, though interrelated, analyses. Each segment will encompass a cluster of related issues to facilitate the exercise. All issues explored in Section B will center on the actions of the belligerents, with an emphasis on State (i.e., Russia's) conduct when functioning as an occupying power.[168] 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 received 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 **refused**. The Russian military then forced Ukrainian MNO employees in the city of Donetsk: (1) to shut down all connectivity to the region; (2) to re-route connectivity via Russian networks; and (3) to install surveillance equipment on local routers, and re-establish

167. *See infra* Part IV Conclusion.

168. 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 89 (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).

consumer connectivity while claiming authority as an occupying force. The MNOs **complied**. Almost immediately, the Russian military authorities began monitoring telecommunications in the region and demanding personal data from internet service providers ("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 permitted only authorized news and entertainment sources to be broadcasted 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 used the telecommunications infrastructure 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 Ukrainian civilian population 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 issued two sets of orders. First, it ordered all MNOs still operating in Ukraine to issue text messages to their subscribers in Donetsk explaining that their mobile phone and internet connections were now censored and unsecure. It further urged them to resist Russian occupation and encouraged downloads of VPNs. The SSSCIP invokes its authority under the recent constitutionally enacted law, which declared a state of emergency, granting it emergency powers that, among other things, allowed it to curtail due process. The MNOs, fearing for employee safety in Donetsk, **refused**. Citing cybersecurity concerns, the SSSCIP then ordered MNOs to disconnect and disable the cell towers, and any transmission of communications services to subscribers in Donetsk. It made clear that if the MNOs did not implement the order immediately, the Ukrainian authorities were prepared to enforce it directly. The MNOs **complied**.

> The SSSCIP issued a second round of orders to the Ukrainian MNOs in Kyiv with the aim of combatting what it denounced as Russian disinformation and war propaganda in the Donetsk region and throughout Ukraine generally. Those orders prohibited MNOs and other ICT operators from enabling, facilitating, or contributing to broadcasting or distributing any content by media sources, entities or bodies identified by SSSCIP as promoting Russian propaganda or disinformation. This included 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 included 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 **complied.**
>
> 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 ordered 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 did. However, given continued skirmishes with pro-Russian factions and 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 **complied.** At the same time, the SSSCIP informed MNOs that it will be installing surveillance equipment like 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 several months after the Russian invasion of Ukraine, Ukrainian mobile network operators ("MNOs") in Kyiv received 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 **refused**. The Russian military then forced Ukrainian MNO employees in the city of Donetsk: (1) to shut down all connectivity to the region; and (2) to re-route connectivity via Russian networks, (3) to install surveillance equipment on local routers, and re-establish consumer connectivity while claiming authority as an occupying force. The MNOs **complied**. Almost immediately, the Russian military authorities began monitoring telecommunications in the region and demanding personal data from ISPs and MNOs on the Ukrainian residents that remained in the city of Donetsk, which they justified as necessary security measures.
>
> ( . . . )
>
> Months later, after protracted fighting, Ukrainian troops and their allies succeeded in retaking the Donetsk region from the Russian occupiers who were forced to retreat back into Russian territory. The SSSCIP immediately ordered 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 did. However, given continued skirmishes with pro-Russian factions and 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 **complied**. At the same time, the SSSCIP informed MNOs that it will be installing surveillance equipment like 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 an international armed conflict.[169] 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."[170] In addition to the basic IHL principles defined in the prior Part (i.e., 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 specific for occupied territories. [171] The duties of the occupying power emanate primarily from the 1907 Hague Convention and its Regulations,[172] the Fourth Geneva Convention, [173] and certain provisions of Additional Protocol I and customary international humanitarian

169. *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. 136 (July 9, 2004); Yoram Dinstein, THE INTERNATIONAL LAW OF BELLIGERENT OCCUPATION (Cambridge Univ. Press 2009).

170. Hague Regulations (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 [https://perma.cc/4RAG-VFDV]; *see also* Kalandarishvili-Mueller, *supra* note 89 (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).

171. *See supra* note 168 and accompanying text.

172. 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 170, 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 [https://perma.cc/6XAC-5BLC]("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*, at 69-93 (Martinus Nijhoff Publisher, 1988)).

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

law.[174] 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.[175]

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.[176] Generally speaking, adverse military forces in occupied territory are bound to "restore law and order and public life" to the furthest extent possible;[177] this means that local laws remain in force except with respect to the occupying power's security.[178] Hence, the occupying power may adopt the measures necessary to ensure the security of its forces in the territory.[179] It is also worth noting 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."[180] Any persons who take up arms to resist occupation will lose their status as civilians and its corresponding protections

174. 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 [https://perma.cc/FS3F-BCS8]. 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* note 169, at ¶ 89.

175. 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 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 [https://perma.cc/6RFQ-A6C7].

176. *See id.*

177. Hague Regulations (IV), *supra* note 170, at art. 43; *See* International Committee of the Red Cross, *How Does Law Protect in War?*, pt. IV. Special Rules on Occupied Territories https://casebook.icrc.org/law/civilian-population#iv_8 [https://perma.cc/CR9B-C5K3].

178. *See* Hague Regulations (IV), *supra* note 170, at Art. 43; Geneva Convention (IV), *supra* note 150, at Art. 64; *How Does Law Protect in War*?, *supra* note 178, pt IV.

179. *Id.*

180. *How Does Law Protect in War?*, *supra* note 177, pt. IV.

under IHL.[181] On a related front, "[p]rivate property cannot be confiscated[,]"[182] except pursuant to "local legislation."[183] Public property and resources can be administered by the occupying power "but only under the rules of usufruct."[184] 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.[185] As the International Committee of the Red Cross ("ICRC") observes:

> [T]he 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.[186]

Returning to the first paragraph of the fact pattern, remember that the mobile network operators based in Kyiv had refused written demands from Russian military officials to shut down connectivity for the oblast province of Donetsk to allegedly protect civilian lives there. Because the Russian occupation in the case study is limited to the Donetsk region, the officials issuing such

---

181. 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. *See* Geneva Convention (IV), *supra* note 150, at art. 4(A)(6). Civilians who engage in such acts surrender their protection as civilians for the duration of their direct participation in hostilities. Protocol I, *supra* note 48, at 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 150, at arts. 4–5; *see also How Does Law Protect in War?*, *supra* note 177.

182. *How Does Law Protect in War?*, *supra* note 177, at IV. Special Rules on Occupied Territories; *Occupation and international humanitarian law: questions and answers*, *supra* note 175; Hague Regulations (IV), *supra* note 170, at art. 46.

183. *How Does Law Protect in War?*, *supra* note 177; Hague Regulations (IV), *supra* note 170, at art. 46.

184. *How Does Law Protect in War?*, *supra* note 177; Hague Regulations (IV), *supra* note 170, at art. 55.

185. *How Does Law Protect in War?*, *supra* note 177.

186. *Id.*

orders did not have the authority to impose their conditions, justified or not, on private ICT actors *outside* that territory who were still bound to respect Ukrainian law and authority.[187] 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 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.[188] It is unlikely 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 seemed tenuous at best. Enabling disinformation and pro-Russian propaganda, as that edict was plainly intended to do, served different purposes altogether, including the central objective of influencing public opinion.[189] That issue is examined under Segment 3.

Whether the second measure—installing surveillance equipment on local routers to monitor the local population—was "necessary" to protect 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 the measure was promulgated.[190] 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.[191]

187. *See supra* notes 212–23 and accompanying text.

188. *See supra* notes 177–78 and accompanying text.

189. *See supra* section III.A.

190. *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 [https://perma.cc/LKE3-BRJ9] ("… 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.").

191 . 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, 100 (NATO CCDCOE; Russell Buchan and Asaf Lubin eds., 2022), https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-

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.[192] On the other hand, 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. [193] Given the volatile climate 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 to help maintain public order.[194] The MNOs were thus justified in complying with Russian demands in this respect (leaving aside for the moment that the MNOs 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

---

Armed-Conflict.pdf [https://perma.cc/J5QR-B9Q8] (lamenting that "[t]he absence of express rights to privacy and data protection in conventional IHL is unlikely to change anytime soon.").

192. Shehabi, *supra* note 191, at 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 462, 462-91 (Robert Kolb, et al. eds., Edward Elgar Publ'g 2022); *see also* EYAL BENAVISTI, THE INTERNATIONAL LAW of OCCUPATION, 96-99 (2006).

193. Shehabi, *supra* note 191, at 99.

194. 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*, *in* THE RIGHTS TO PRIVACY AND DATA PROTECTION IN TIMES OF ARMED CONFLICT 12, 12 (Russell Buchan & Asaf Lubin eds., NATO CCDCOE Publ'n 2022), https://ccdcoe.org/uploads/2022/06/The-Rights-to-Privacy-and-Data-Protection-in-Armed-Conflict.pdf [https://perma.cc/MXZ6-AF37]. For a number of reasons, many of them outlined throughout this article, I find such arguments unpersuasive.

this dynamic can apply only to "certain types of activity."[195] The question for our purposes, therefore, is this: do existing and emerging norms of IHRL apply in the Russian-occupied territory of Ukraine to fill the pertinent lacunae left by IHL specifically with respect to the data privacy rights of the civilian population? The answer 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 encompassed only non-derogable human rights, which do not include privacy or freedom of expression.[196] Even if it was assumed there was concurrent application of IHRL without derogation and IHL, there were still substantive obstacles in attempting to extrapolate data privacy protections from IHRL to supplement IHL 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."[197] They are especially "inapposite in the context of military occupation."[198] 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."[199]

195. OCCUPATION AND OTHER FORMS OF FOREIGN ADMINISTRATION OF TERRITORY, *supra* note 170, at 8.

196. *See supra* notes 42, 67–68 and accompanying text.

197. *See* HOW DOES LAW PROTECT in WAR?, *supra* note 177 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.").

198. Shehabi, *supra* note 191, at 103.

199. Shehabi, *supra* note 191, at 105-06.

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 III, *supra*, established that both the ICCPR and ECHR apply extraterritorially to State parties' actions in just this way.[200] This means that in addition to the IHL obligations incumbent upon Russian forces in occupied Donetsk,[201] 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.[202] Might this be the avenue for filling the IHL lacunae? Probably not.

Russia's poor human rights record at home,[203] together with its flouting of the laws of war in Ukraine[204] 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).[205] In the case study segment, 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.[206] If nothing else, this paradox demonstrates the practical limits of

200. *See supra* notes 39–40 and accompanying text.

201. *See supra* notes 48, 91–92 and accompanying text.

202. *See* HOW DOES LAW PROTECT in WAR?, *supra* note 179, at ICJ/Israel, Separation Wall/Security Fence in the Occupied Palestinian Territory, ¶¶ 102–11, https://casebook.icrc.org/case-study/icjisrael-separation-wallsecurity-fence-occupied-palestinian-territory#part [https://perma.cc/V45J-U2BP].

203. *See supra* note 101 and accompanying text.

204. *See supra* note 90 and accompanying text.

205. *See infra* notes 90–92 and accompanying text. To be clear, I am not arguing that human rights law would not apply in Russian occupied territory; it does, due to Russia's (assumed) control of that territory. *See supra* note 40 and accompanying text (discussing the extraterritorial reach of the ICCPR under such circumstances). But given the realities of the armed conflict in Ukraine, and Russia's handling of the war at home and abroad, any attempt to demand *compliance* by Russia's occupying forces with human rights norms as a practical or strategic matter borders on quixotic.

206. *See generally, supra* notes 64–67, 90–92 and accompanying text. (The paradox is that Ukrainians in occupied territory enjoy greater protection from Russian law than under their own).

international law and human rights in times of war. A better response would be 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.[207]

The foregoing helpfully advances the analysis of a related but separate question raised in Segment 1: were the Russian orders intended to maintain public order consistent with "local law" as seen in the final paragraph of the case study? Would domestic law have permitted the imposition of the same restrictive measures by Ukrainian forces after recuperating the once occupied territories and operating under 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,[208] 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 like 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 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 the earlier discussion of the legal frameworks operating in Ukraine, which has derogated from its principal human rights obligations under the ICCPR and the ECHR.[209] There can be little doubt that the constitutionally-enacted emergency legislation was justified and thus legitimate.[210] That war-time legislation in turn authorized action under domestic and international law to impose even onerous restrictions on privacy rights and freedom of expression,

207. *See infra* note 245 and accompanying text.

208. *See infra* notes 213–20 and accompanying text (discussing the duties of States under international law with respect to international telecommunications infrastructure).

209. *See supra* note 41 and accompanying text.

210. *See id.*

which in peace-time would enjoy robust constitutional and legal protections.[211] 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 were not on their face or implemented in arbitrary or discriminatory manner, they are presumed to be valid.[212] And if such restrictions are most likely valid when adopted by Ukrainian authorities under their domestic 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.[213] 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 issued two sets of orders. First, it ordered all MNOs still operating in Ukraine to issue text messages to their subscribers in Donetsk explaining that their mobile phone and internet connections were now censored and unsecure. It further urged them to resist Russian occupation, and encouraged download of VPNs. The SSSCIP invoked its authority under the recent constitutionally enacted law, which declared a state of emergency, granting it emergency powers that, among other things, allowed it to curtail due process. The MNOs, feared for employee safety in Donetsk, and **refused**. Citing cybersecurity concerns, the SSSCIP then ordered MNOs to disconnect and disable the cell towers, and any transmission of communications services to subscribers in Donetsk. It made clear that if the MNOs did not

211. *See supra* notes 41–42 and accompanying text.

212. *See supra* notes 41–42 and accompanying text. This means that the three-part test will not apply.

213. *See supra* note 196 and accompanying text.

> implement the order immediately, the Ukrainian authorities were prepared to enforce it directly. The MNOs **complied**.

International law today establishes that States as a function of their sovereignty must maintain and safeguard international telecommunications infrastructure on their territory, both public and private.[214] 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."[215] 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."[216] 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."[217] 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."[218] The International Group of Experts who prepared the Tallinn Manual 2.0, in its commentary to these rules, clarified that this authority "encompasses suspension of incoming

---

214. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, ch. 11, rule 61 at 288 (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.

215. GGE 2015 REPORT, *supra* note 134, at ¶ 27; GGE 2019-2021 REPORT, *supra* note 135, at ¶ 71(b).

216. GGE 2019-2021 REPORT, *supra* note 134, at ¶ 71(b).

217. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, *supra* note 214, ch. 11, rule 61 commentary ¶¶ 5, 7 at 289-90.

218. *Id.*, ch.11, rule 62 commentary ¶1 at 291-92.

and outgoing communications, as well as those that transit a State's territory."[219] 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.[220] It is important to highlight that these IHL rules are derived from the existing treaty regime established by the International Telecommunications Union ("ITU")[221] 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."[222] 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.[223]

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. For example, the Tallinn 2.0 Experts' view that the Egyptian authorities' 2011 shutdown of international internet and mobile telephony in response to the civil uprising resulting from the "Arab Spring" was authorized under this framework.[224] If true, turning back to the case study, it is

219. *Id.*, ch.11, rule 62 commentary ¶3 at 292-93.

220. *Id.*, ch.11, rule 62 commentary ¶1 at 291-92.

221. *Id.*, ch.11, rules 61-62 commentary at 288-94.

222. *Id.*, ch. 11 ¶9 at 287. 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: Protecting Civilians from Disinformation During Armed Conflict*, 914 INT'L REV. OF THE RED CROSS 659, 681-82 (2021).

223. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, *supra* note 214, ch. 11 ¶9 at 287.

224. *Id.*, ch.11, rule 62 commentary ¶4 at 293. 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*

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, 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.[225]

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.[226] 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 and 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.[227] 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 cyber-security.[228]

A skeptic could challenge Segment 2's analysis 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 this issue. The GGE has stressed, when affirming State prerogatives emanating from

---

*Internet Shutdown that Rocked Egypt*, ACCESS NOW (Jan. 21, 2016, 7:35 PM), https://www.accessnow.org/five-years-later-the-internet-shutdown-that-rocked-egypt/ [https://perma.cc/W74A-N52P].

225. *See supra* note 216 and accompanying text.

226. *See supra* note 85 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.

227. *See supra* note 85 and accompanying text.

228. *See supra* notes 213–24 and accompanying text.

sovereignty, that "[e]xisting obligations under international law are [also] applicable to States' ICT-related activity."[229] Such obligations include those to "respect and protect the human rights of individuals over whom they exercise control."[230] The Ukrainian State's power here is thus limited by any IHRL obligations it has "shoulder[ed] prohibiting it from doing so in [a particular] case."[231] The Tallinn 2.0 Experts recognized this feature of the legal regime when finding that Egypt's temporary shutdown of telecommunications complied with the pertinent international obligations; they caveated their conclusion by stating that it was proffered "without prejudice to the question of whether Egypt's action[s] complied with . . . respect for the international human right to freedom of expression,"[232] which they almost certainly did not.[233]

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.[234] 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

229. GGE 2015 REPORT, *supra* note 134, at ¶ 28(b); GGE 2019-2021 REPORT, *supra* note 136, at ¶ 71(b).

230. Schmitt, *supra* note 133.

231. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS, *supra* note 214, ch. 11, rule 62 commentary ¶ 1 at 291-92.

232. *Id.,* ch. 11, rule 62 commentary ¶ 4 at 293.

233. *See, e.g.,* WOLFGANG BENEDEK & MATTHIAS C. KETTEMEN, FREEDOM OF EXPRESSION AND THE INTERNET §6.2.1 (Council of Europe Publishing 2013) ("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.").

234. *See supra* notes 43, 65–68 and accompanying text.

especially true given the features of the international armed conflict reflected in the case study, together with the appropriate operation of *lex specialis.*[235]

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 a manner consistent with the State's duty to protect its population under both IHL and IHRL.[236] In this vein, urgent government communications to protect national security and public order must be given priority in times of war as well as peace.[237] Only with respect to the second set of orders would freedom of expression be reasonably implicated such as concerns about 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, wartime 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.[238] An alternative approach with a similar outcome is provided by the operation of *lex specialis*, which would require the direct application of the

235. *See* prior discussion of *lex specialis* and the concurrent application of IHL and IHRL, *supra* notes 71–75 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 (2014); Office of the High Comm'r on Human Rights, *The International Legal Protection of Human Rights in Armed Conflict*, U.N. Doc. HR/PUB/11/01, at 54-70 (2011).

236. 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; *see* 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 150, at art. 4 (protecting those who "find themselves . . . in the hands of a Party to the conflict . . . of which they are not nationals.").

237. *See supra* notes 221–22 and accompanying text.

238. *See supra* note 36 and accompanying text. *See also* Benedek & Kettemen, *supra* 235 ("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 be proportionate, in order to safeguard the lives of others, to introduce brief regional Internet shutdowns as an *ultima ration*.").

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.[239] 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 broadcasted 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 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 Ukrainian civilian population more broadly regarding Russia's valiant efforts to "liberate" the country from "fascism" and foreign influences.
>
> ( . . . )
>
> The SSSCIP issued a second round of orders to the Ukrainian MNOs in Kyiv with the aim of combatting what it denounced as Russian disinformation and war propaganda in the Donetsk region and throughout Ukraine generally. Those orders prohibited MNOs and other ICT operators from enabling, facilitating, or contributing to broadcasting or distributing any content by media sources, entities or bodies identified by SSSCIP as promoting Russian propaganda or disinformation. This included 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 included those

239. *See supra* notes 71–72 and accompanying text.

> 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 **complied**.

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.[240] Strictly speaking, neither is prohibited by the laws of armed conflict.[241] 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.[242] 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.[243] Indeed, these traditional IHL rules are widely seen as outmoded given modern advances in ICTs and the cyber operations they enable.[244] For this reason, a growing number of commentators are clamoring for greater and more specific regulation of information operations in war time.[245] 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

240. *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/ [https://perma.cc/SG5B-FP7T] (general discussion on the nature of modern disinformation); *see* Katz, *supra* note 222 (thorough analysis of disinformation in the context of armed conflict). For a thorough analysis of disinformation.

241. Robin Geiss & Henning Lahmann, *Protecting the Information Space in Times of Armed Conflict,* JUSTSECURITY (Mar. 3, 2021), https://www.justsecurity.org/75066/protecting-the-information-space-in-times-of-armed-conflict/ [https://perma.cc/V5W6-PSU9]; *see also* Katz, *supra* note 222, at 662.

242. International Committee of the Red Cross, *supra* note 27, at rule 57.

243. International Committee of the Red Cross, *supra* note 27, at rule 65.

244. Geiss & Lahmann, *supra* note 242; *see* Katz, *supra* note 222.

245. Geiss & Lahmann, *supra* note 242; *see* Katz, *supra* note 222.

> 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.[246]

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 seen 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.[247] 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.[248] Russian propaganda and misinformation transmitted from the commandeered telecoms infrastructure were calibrated to influence if not "control the narrative regarding the conflict"[249] within Donetsk, as well as throughout the rest of Ukrainian territory not under occupation.

IHL does not prohibit such information operations targeting public opinions.[250] Indeed, on these facts, none of the Russian occupiers' actions would transgress the emerging principles on inciting violence against protected persons and objects, or otherwise harming the well-being of the civilian population, through the use of disinformation tactics in wartime.[251] It follows as well that this reasoning applies to the countermeasures adopted

246. 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/ [https://perma.cc/PB6Q-CFNH].

247. *See supra* notes 170–86 and accompanying text.

248. *See supra* notes 190–199 and accompanying text.

249. Katz, *supra* note 222, at 661.

250. *See supra* notes 243–44 and accompanying text.

251. *See* Katz, *supra* note 222, at 660, 668.

by their Ukrainian adversaries to combat the disinformation operations, so long as those measures are not themselves otherwise prohibited by IHL.[252] 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 were 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 mirrored its brutal repression of free speech at home, which has been categorically criticized for transgressing human rights.[253] But, IHRL does not apply fully to the Donetsk region, a war zone.[254] 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.[255] Under "local" Ukrainian law amended by the state of emergency legislation, derogation operates to leave only a handful of non-derogable rights in effect.[256] However, the freedom of expression or the press was not included; thereby, opening the door to informational policies and practices by the belligerents that do not otherwise violate IHL (e.g., perfidy, or war crimes) or international criminal law (e.g., genocide or crimes against humanity).[257] 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.[258] But even then, as the analysis of IHRL

252. *See supra* notes 241–44 and accompanying text.

253. *See supra* notes 99–102 and accompanying text.

254. *See supra* notes 190–199 and accompanying text.

255. *See supra* notes 43, 66–69, 71 and accompanying text;; *see also* Katz, *supra* note 223, and accompanying text, at 672, 682.

256. *See supra* notes 43, 67–68, 70 and accompanying text.

257. *See supra* note 255 and accompanying text.

258. *See supra* notes 205–07 and accompanying text (citing discussion of paradox created by the scenario).

below indicates, it is far from clear that such claims would result in a different outcome.[259]

Assuming for argument's sake 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? As previously discussed, the two bodies of law are held to apply concurrently and, ideally, to complement each other.[260] But what does that 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 integrity, and personal liberty.[261] 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

259. *See infra* notes 264–89 and accompanying text.

260. International Committee of the Red Cross, *supra* note 27, at 8.

261. International Committee of the Red Cross, *supra* note 27; *See also* Sassòli et al., *supra* note 145, at II. Protected Rights.

> "sovereign", while respect for IHL can be considered as a treatment conceded by the "sovereign".[262]

Whether 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.[263] 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.[264] 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.[265] Similarly, the right of communication is reserved for both POWs and civilians in occupied territories;[266] 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:

---

262. Sassòli et al., *supra* note 145, at III. Implementation.

263. Sassòli et al., s*upra* note145; *see also supra* text accompanying note 57.

264. Sassòli et al., s*upra* note 145; *see also supra* text accompanying note 57 (suggesting IHRL fills that gap where IHL is silent).

265. Geneva Convention (III) Relative to the Treatment of Prisoners of War, art. 4, Aug. 12, 1949, T.I.A.S. No. 3364, 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 [https://perma.cc/7294-NFVX] [hereinafter Geneva Convention (III)]; War correspondents are entitled to embed in the armed forces and are accorded POW status if captured. *Id.*

266. *See id.*, art. 71; Geneva Convention (IV), *supra* note 150, 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* Geneva Convention (III), *supra* note 265, art. 76; and Geneva Convention (IV), *supra* note 150 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.

> 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 online or offline except in accordance with the requirements of articles 19(3) and 20(2) of the [ICCPR], strictly and narrowly construed.[267]

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.[268] 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."[269] It became 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.[270]

The clearest example of this is ICCPR Article 20(1), that the UN Special Rapporteur does not mention, which prohibits any "propaganda for war," a norm that by definition can only apply in times of peace.[271] 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 . . . ,"[272] alluding to inherent limits arising in and around international

---

267. Khan, *supra* note 86, at 18 ¶ 88.

268. U.N. Human Rights Comm., Int'l Covenant on Civil and Human Rights, General Comment No. 34, art. 19: Freedoms of Opinion and Expression, UN Doc. CCPR/C/GC/34 ¶ 22 (2011).

269. ICCPR, *supra* note 36, at art. 20.

270. Sassòli et al., *supra* note 145, at III. Implementation.

271. *See, e.g.,* Off. of the UN High Comm'n for Hum. Rts. (OHCHR), *GENERAL COMMENT NO. 11, Prohibition of Propaganda for War and Inciting National, Racial or Religious Hatred (Art. 20)*, CCPR/C/GC/11 (Sept. 7, 1983). 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.

272. *See id*. at 1 ¶ 2.

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.[273] Under extreme circumstances like those arising during a devastating cyber-attack, internet shutdowns could conceivably even be necessary to protect civilians and essential civilian infrastructure.[274] To round out the point, let us return to 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 assuming that IHRL applies in Ukraine without derogation, there is a situation similar to the one confronted by the European Union in its series of resolutions imposing sanctions on select Russian media outlets for similar reasons.[275] The framework outlined in the quote above from the UN Special Rapporteur was the very framework used to analyze the legitimacy of the EU sanctions adopted in response to Russian disinformation, and, as a result, found them lacking under human rights law.[276] It is also the one that governs in the Segment 3 hypothetical. Similar to the case with the European Union's sanctions, the proposed Ukrainian restrictions would have to be evaluated using 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.[277] Under this approach, "the armed conflict [functions] primarily as context and a critical source of factual inputs for [the] analysis,"[278] 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

273. *See supra* notes 218–25 and accompanying text.
274. *See supra* notes 222–24 and accompanying text.
275. *See supra* notes 104–11 and accompanying text.
276. *See supra* notes 112–13 and accompanying text.
277. *See* Khan, *supra* note 86, at 6–8, ⁋⁋ 30–40.
278. Carrillo, *supra* note 166.

democracies rapidly becomes evident.[279] The European Union'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 twenty-seven EU countries that their actions are "consistent with the fundamental rights and . . . in particular with the right to freedom of expression and information."[280]

One cannot help but wonder whether those critics would find the Ukrainian government's restrictions in Segment 3, which are expressly modeled on the European Union'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 European Union, and thus would ultimately tip the scales in its favor. But the question remains: did the critics of the European Union's sanctions on Russian media give proper weight to the "armed conflict as [the] context and a critical source of inputs" when analyzing the measures imposed under the IHRL "three-part" test for legitimate limits on freedom of expression? There is reason to believe they did not.[281] In any event, the impact of armed conflict in the digital age on non-belligerent States 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 ensured that in the circumstances of the case study as originally presented, even onerous censorship measures like these can legitimately be

279. *See, e.g.*, Shehabi, *supra* note 192, at 102–03 (explaining that IHRL approaches to data privacy "rests on a theory of *procedural democracy* which is inapposite in the context of military occupation") (emphasis in original).

280. *See supra* note 108 and accompanying text; *see also* Carrillo, *supra* note 166.

281. *See* The Court of Justice of the European Union confirmed that the three-part test was properly applied by the EU Member States. Court of Justice of the European Union Press Release No. 132/22, Judgment of the General Court in Case T-125/22 (July 27, 2022), https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-07/cp220132en.pd [https://perma.cc/GJ9N-UN88].

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 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*.

## *V. CONCLUSION*

Recall the overarching inquiries highlighted in the Introduction: what is an ICT company to do when operating during an international armed conflict like the one raging in Ukraine? How should technology company executives respond to urgent government demands—often conflicting—to propagate or censor online content arising in the context of war, including

282. *See supra* notes 43, 66–69 and accompanying text.

283. *See* Katz, *supra* note 240, at 931–932; *see also* Shehabi, *supra* note 191, at 96–100 .

284. *See* Shehabi, *supra* note 191, at 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.").

285. *See supra* notes 241–45 and accompanying text.

286. *See, e.g.*, Katz, *supra* note 223 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* O'Connell, *supra* note 195, at 28.

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 studies 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

287. *Global Conflict Tracker*, COUNCIL ON FOREIGN RELATIONS, https://www.cfr.org/global-conflict-tracker [https://perma.cc/6YGY-Q53J](last visited Aug. 28, 2022).

288. Global Network Initiative, Submission to the Special Rapporteur Report on Freedom of Expression in times of Armed Conflict and other Disturbances, at 6,

sentiments of the UN Special Rapporteur on Freedom of Expression that progress in confronting these outstanding issues will require "the proactive engagement of States, companies, international organizations, civil society, and the media. The need for multi-stakeholder dialogue and partnerships cannot be overstated."[289]

https://globalnetworkinitiative.org/wp-content/uploads/2022/07/GNI-FoE-Conflict-Submission-12July22-1-2.pdf [https://perma.cc/66N5-SLLE].

289. Khan, *supra* note 86, at 18 ¶87.