United Nations A/77/288

General Assembly

Distr.: General
12 August 2022

Original: English

Seventy-seventh session
Item 69 (b) of the provisional agenda*
Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms

Disinformation and freedom of opinion and expression during armed conflicts**

Note by the Secretary-General

The Secretary-General has the honour to transmit to the General Assembly the report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, submitted in accordance with Human Rights Council resolution 43/4.

* A/77/150.

** The present report was submitted after the deadline in order to reflect the most recent information.

22-12580 (E) 300822

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Summary

In the present report, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, examines the challenges that information manipulation poses to freedom of opinion and expression during armed conflict. In the report, she notes that the information environment in the digital age has become a dangerous theatre of war in which State and non-State actors, enabled by digital technology and social media, weaponize information to sow confusion, feed hate, incite violence and prolong conflict.

Emphasizing the vital importance of the right to information as a "survival right" on which people's lives, health and safety depend, the Special Rapporteur recommends that human rights standards be reinforced alongside international humanitarian law during armed conflicts. She urges States to reaffirm their commitment to upholding freedom of opinion and expression and ensuring that action to counter disinformation, propaganda and incitement is well grounded in human rights. She recommends that social media companies align their policies and practices with human rights standards and apply them consistently across the world. She concludes by reiterating the need to build social resilience against disinformation and promote multi-stakeholder approaches that engage civil society as well as States, companies and international organizations.

Contents

I. Introduction

1. During armed conflict, people are at their most vulnerable and in the greatest need of accurate, trustworthy information to ensure their own safety and well-being. Yet, it is precisely in those situations that their freedom of opinion and expression, which includes "the freedom to seek, receive and impart information and ideas of all kinds",[1] is most constrained by the circumstances of war and the actions of the parties to the conflict and other actors to manipulate and restrict information for political, military and strategic objectives.

2. Manipulation of information and the information environment by State and armed groups has long been a feature of war. It has taken many forms, from "ruses of war" that seek to deceive and demoralize enemy troops to "information operations" aimed at influencing the public and "hate speech" aimed at fomenting violence against minorities. What is new and of serious concern is the ease, scale and speed with which false or misleading harmful information is being created, distributed and amplified by digital technology.

3. Social media platforms play a dual role in modern conflicts. On the one hand, they enable people to remain connected to family, friends and the outside world and to access a wide range of critical life-saving information. On the other hand, they serve as vectors of disinformation, propaganda and hate speech.

4. Either in response to disinformation or as part of their own efforts to manipulate information, many States have sought to restrict access to information through laws on national security, counter-terrorism or "false news", attacks on independent journalists and human rights defenders, closure of independent media outlets, Internet shutdowns, and regulation of digital platforms in ways that undermine human rights and aggravate the very problems they wish to address.

5. Freedom of opinion and expression is not part of the problem. It is the means by which to combat disinformation and a value in itself. Access to diverse, verifiable sources of information is a fundamental human right. It is an essential necessity for people in conflict-affected societies. In effect, it is a "survival right". It is also vital for resolving conflicts, exposing human rights abuses and seeking justice and accountability.

6. The heightened risks that disinformation and other forms of information manipulation pose to civilian populations, especially marginalized and vulnerable groups, and to human rights, humanitarian operations and peace processes underscore the urgency to reaffirm the obligations of States and companies to uphold freedom of opinion and expression. It is through respect for human rights and humanitarian principles that the integrity of information as well as the safety of people can be maintained during armed conflict.

7. Building on her report on countering disinformation while promoting and protecting freedom of opinion and expression,[2] in the present report, the Special Rapporteur focuses on disinformation, propaganda and advocacy of hatred that constitutes incitement to discrimination, hostility or violence ("hate speech") in the context of armed conflicts, as defined under international humanitarian law.

8. In the report, the Special Rapporteur examines the nature and impact of information manipulation; the legal framework; and the roles of States and social media companies. She identifies challenges and threats, including areas of weak compliance or legal uncertainties, as well as good practices, and makes recommendations, mainly to States and social media companies. The report is not a

[1] Article 19 (2), International Covenant on Civil and Political Rights.

[2] A/HRC/47/25.

comprehensive study and does not examine the role of armed groups or companies other than social media, or cyberoperations.

9. The Special Rapporteur acknowledges the complex and sensitive nature of the subject and the need for further research, analysis and consultations and considers the report a preliminary step in engaging with interested stakeholders.

10. The report has benefited from consultations and written submissions from States, journalists, human rights defenders, scholars and civil society organizations.[3]

II. Concepts, victims and vectors

A. Conceptual challenges

11. Despite growing interest in information manipulation and the adoption of United Nations resolutions on disinformation,[4] there remains considerable confusion about the various concepts and how they relate to each other. The lack of international agreement on definitions underscores the complexity of the notions and the polemics surrounding them.

12. Disinformation, propaganda and advocacy to incite discrimination, violence and hostility share some common features: lack of clear, agreed definitions; high prevalence in disturbances and conflict settings; amplification by digital technology; increasing focus on civilian populations rather than military personnel; and detrimental impact on human rights, democracy and peace processes. The concepts overlap at times. For instance, some forms of disinformation and propaganda can amount to advocacy of incitement to violence, hostility, discrimination and war crimes.

13. All three concepts contain some degree of manipulation, deception and distortion of information that is meant to create confusion, including about their own meaning. Factual information is delegitimized as "fake news" or disinformation. Opinions, beliefs and uncertain knowledge are distorted to discredit the source. False information is instrumentalized to cause harm. Verifiable data from international bodies, including reports of the United Nations independent experts, are dismissed as disinformation, while propaganda is promoted as facts.

14. Disinformation has been present for millenniums but has gained new currency in the digital age. While there is no single agreed definition of disinformation, the term is used increasingly to signify the manipulation of false or misleading information to intentionally deceive and cause public harm.[5] It should be distinguished from misinformation, which is falsehood disseminated with no intent to cause harm.

15. Propaganda is mentioned but not defined in international law.[6] While disinformation seeks to confuse and disrupt, the objective of propaganda is to advance a particular agenda or party. Derived from the notion of "propagating" or spreading information and views, it has a pejorative sense of disseminating information that may be true or false but is biased, partial, misleading and emotive.[7] Propaganda and disinformation may overlap as part of "information operations", which are commonly understood as campaigns by States or political actors to influence the views, attitudes and behaviour of adversaries or the public in order to achieve political and military objectives.

---

[3] The submissions are available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression.

[4] General Assembly resolution 76/227 and Human Rights Council draft resolution A/HRC/49/L.31/Rev.1; see also A/HRC/47/25.

[5] See European Commission, Strengthened Code of Practice on Disinformation, available at https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation.

[6] Article 20 (1) of the International Covenant on Civil and Political Rights.

[7] See Manfred Nowak, *U.N. Covenant on Civil and Political Rights CCPR Commentary* (Kehl am Rhein, Germany, N.P. Engel, 1993).

16. Incitement, or the act of directly or indirectly urging or instigating the commission of a crime, is prohibited in international law. The term "incitement" is used in the present report to denote advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility, violence (commonly referred to as "hate speech"), war crimes, crimes against humanity and genocide.

B. People and issues at risk

17. There is growing evidence that information is being manipulated to trigger, aggravate and sustain violence over prolonged periods, increasing the fog of war with contradictory and false news and fostering a climate of distrust. The dynamics of armed conflict and disinformation work in a complex interplay with other grievances to exacerbate human suffering, feed hatred and target vulnerable groups.

18. **Minorities and marginalized groups**. From Rwanda[8] three decades ago to Myanmar[9] and Ethiopia[10] in more recent times, parties to a conflict have used mass communications platforms to whip up hatred among the population, dehumanize the other side and incite gross violations of human rights, war crimes, crimes against humanity and genocide.[11] In some situations, political leaders have used intolerant, divisive and dangerous rhetoric to deny established facts, raise tensions and scapegoat national, ethnic and religious groups.[12] Refugees, internally displaced persons and migrants have been portrayed often as threats to national security or social cohesion to drum up animosity against them.[13]

19. Online hate speech and incitement in the Central African Republic have helped to fuel cycles of atrocities between Christians and Muslims in recent years.[14] In Ethiopia, online "activists" have used their Facebook accounts to spread hate and incite attacks, killings and displacement of other tribes.[15] In Iraq, militant groups use

[8] See Montreal Institute for Genocide and Human Rights Studies, "Rwanda radio transcripts", available at https://www.concordia.ca/research/migs/resources/rwanda-radio-transcripts.html.

[9] A/HRC/39/CRP.2; see also submission of Free Expression Myanmar.

[10] See Jasper Jackson and others, "Facebook accused by survivors of letting activists incite ethnic massacres and misinformation in Ethiopia", Bureau of Investigative Journalism, 20 February 2022, available at https://www.thebureauinvestigates.com/stories/2022-02-20/facebook-accused-of-letting-activists-incite-ethnic-massacres-with-hate-and-misinformation-by-survivors-in-ethiopia.

[11] See SC/14939.

[12] See Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression and others, "Joint Declaration on Politicians and Public Officials on Freedom of Expression", available at https://www.ohchr.org/sites/default/files/2022-04/Joint-Declaration-2021-Politicians_EN.pdf.

[13] See https://www.un.org/en/hate-speech/impact-and-prevention/targets-of-hate.

[14] See Nicola Barrach-Yousefi and others, *A Lexicon of Hateful and Inflammatory Speech in the Central African Republic* (PeaceTech Lab, Washington, D.C.), available at https://static1.squarespace.com/static/54257189e4b0ac0d5fca1566/t/60edb60d3680ef421b572ff7/1626191378524/CARLexicon_English_web.pdf; see also https://www.ungeneva.org/fr/news-media/news/2022/07/rca-un-expert-de-lonu-alarme-par-la-proliferation-des-fausses-informations.

[15] See Global Witness, "Now is the time to kill: Facebook continues to approve hate speech inciting violence and genocide during civil war in Ethiopia", 9 June 2022, available at https://www.globalwitness.org/en/campaigns/digital-threats/ethiopia-hate-speech/; see also Tessa Knight and Beth Alexion, "Influential Ethiopian social media accounts stoke violence along ethnic lines", DFRLab, 17 December 2021, available at https://medium.com/dfrlab/influential-ethiopian-social-media-accounts-stoke-violence-along-ethnic-lines-6713a1920b02.

Telegram, Facebook and YouTube to propagate hate and division along sectarian lines, forcing many of the targets, especially women, to hide or flee their homes.[16]

20. The wave of violence and killings that followed the shooting of singer Hachalu Hundessa is just one illustration of how online hate translates into offline atrocities.[17] In South Sudan, derogatory language was used online to stigmatize pastoralist Dinka tribes as threats to territorial and ethnic integrity and incite fighters and armed groups to identify, attack and kill them.[18]

21. **Civilian populations**. Disinformation about the location and nature of hostilities, the displacement of troops or population, or the existence and accessibility of safe areas can lead people to make wrong and dangerous decisions. In many situations, civilians find themselves affected not only by disinformation but also by information blackouts and Internet shutdowns imposed by the authorities.[19] When families cannot communicate with one another, when people cannot access reliable information about the security situation or the availability of essential services or humanitarian assistance, they are unable to assess the risks to their security and safety and make decisions accordingly. Civilians in Ethiopia have described the lack of access to reliable information as turning their lives "upside down".[20] The importance of reliable information about humanitarian corridors was highlighted in the case of civilians trying to escape the fighting in Mariupol, Ukraine.[21]

---

[16] See Joey Shea and Ruba al-Hassani, "Hate speech, social media and political violence in Iraq: Virtual civil society and upheaval", The Tahrir Institute for Middle East Policy, 11 February 2021, available at https://timep.org/commentary/analysis/hate-speech-social-media-and-political-violence-in-iraq-virtual-civil-society-and-upheaval/; see also Pshtiwan Faraj and Emilie Wilson, "Deeply ingrained prejudice fuels hate speech in Iraq", Institute of Development Studies, 9 January 2021, available at https://www.ids.ac.uk/opinions/deeply-ingrained-prejudice-fuels-hate-speech-in-iraq/.

[17] See United Nations press release, "UN experts call on Ethiopia to allow peaceful protests, welcome partial restoration of Internet", 21 July 2020, available at https://www.ohchr.org/en/press-releases/2020/07/un-experts-call-ethiopia-allow-peaceful-protests-welcome-partial-restoration?LangID=E&NewsID=26115.

[18] See Dangerous Speech Project, "Dinka called 'MTN' in South Sudan", 2 January 2022, available at https://dangerousspeech.org/dinka-called-mtn-in-south-sudan/; see also Community Power for Progress Organization, "Social networks ignite the war that puts the country on the brink of genocide", 15 May 2017, available at http://cepo-southsudan.org/news/social-networks-ignite-war-puts-country-brink-genocide.

[19] Joint submission of Mass Media Defence Centre, Memorial Human Rights Defence Centre, Net Freedoms Project and OVD-Info.

[20] See Report of the Ethiopian Human Rights Commission/Office of the United Nations High Commissioner for Human Rights (OHCHR) Joint Investigation into Alleged Violations of International Human Rights, Humanitarian and Refugee Law Committed by all Parties to the Conflict in the Tigray Region of the Federal Democratic Republic of Ethiopia, available at https://digitallibrary.un.org/record/3947207?ln=en.

[21] Deutsche Welle, "Ukraine says planned Mariupol evacuations fell short – as it happened", April 2022.

22. Studies have shown the disproportionate impact of disinformation on women,[22] children[23] and LGBTIQ+ persons.[24] Their situation is only worsened in conflict settings, where support is often lacking.

23. Distorted situational awareness can significantly increase anxiety, fear and stress and, combined with trauma resulting from exposure to violence and atrocities, can have prolonged consequences for mental health.[25] By constantly stimulating feelings of anger and outrage, disinformation can also instigate radical forms of resentment, extreme opinions and resort to violence.

24. **Human rights and humanitarian actors**. Parties to the conflict or their allies have used disinformation and propaganda to discredit human rights defenders and humanitarian actors and disrupt humanitarian access and assistance. For example, in Ukraine,[26] the Syrian Arab Republic[27] and the State of Palestine,[28] orchestrated disinformation campaigns have spread unfounded accusations against the organizations of partiality, criminal activities or links with armed groups.

25. Such disinformation can affect people's perception of these organizations and induce them to refuse to engage with them or accept their services. Smear campaigns can affect donor funding and create security risks, including the risk of gender-based violence against female workers, affecting the presence, access and ability of humanitarian workers to provide assistance to vulnerable populations.[29] In some situations, such as in Ethiopia, the authorities have restricted or blocked the work of humanitarian organizations, accusing them of spreading disinformation when their activities or communications did not align fully with the interests of the governments.[30]

---

[22] EU DisinfoLab, "Gender-based disinformation: Advancing our understanding and response", 20 October 2021, available at https://www.disinfo.eu/publications/gender-based-disinformation-advancing-our-understanding-and-response/; see also Lucina Di Meco and Kristina Wilfore, "Gendered disinformation is a national security problem", Brookings Institution, 8 March 2021, available at https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/.

[23] See United Nations Children's Fund (UNICEF) Office of Global Insight and Policy, "Digital misinformation/disinformation and children", August 2021, available at https://www.unicef.org/globalinsight/media/2096/file/UNICEF-Global-Insight-Digital-Mis-Disinformation-and-Children-2021.pdf.

[24] See European Parliament, Directorate-General for External Policies, Policy Department, "Disinformation campaigns about LGBTI+ people in the EU and foreign influence", July 2021, available at https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/653644/EXPO_BRI(2021)653644_EN.pdf.

[25] See Eian Katz, "Liar's war: Protecting civilians from disinformation during armed conflict" in *International Review of the Red Cross*, No. 914, December 2021, available at https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914.

[26] See International Committee of the Red Cross (ICRC), "Ukraine: Addressing misinformation about ICRC's activities", 26 March 2022, available at https://www.icrc.org/en/document/ukraine-addressing-misinformation-about-icrcs-activities.

[27] See Mel Bunce, "Humanitarian communication in a post-truth world" in *Journal of Humanitarian Affairs*, Manchester openhive, Vol. 1, No. 1, 1 January 2019, available at https://www.manchesteropenhive.com/view/journals/jha/1/1/article-p49.xml; see also Louisa Loveluck, "Russian disinformation campaign targets Syria's beleaguered rescue workers" in The Washington Post, 18 December 2018, available at https://www.washingtonpost.com/world/russian-disinformation-campaign-targets-syrias-beleaguered-rescue-workers/2018/12/18/113b03c4-02a9-11e9-8186-4ec26a485713_story.html.

[28] Submission of Charity and Security Network (2021 call for submissions).

[29] See Rachel Xu, "You can't handle the truth: misinformation and humanitarian action", ICRC Humanitarian Law and Policy Blog, 15 January 2021, available at https://blogs.icrc.org/law-and-policy/2021/01/15/misinformation-humanitarian/.

[30] See Kaamil Ahmed, "Ethiopia suspends aid groups for 'spreading misinformation'" in *The Guardian*, 6 August 2021, available at https://www.theguardian.com/global-development/2021/aug/06/ethiopia-suspends-aid-groups-for-spreading-misinformation.

26. **Public trust**. Disinformation creates public distrust in the integrity of information, which in turn has broad social and political implications, hindering peace, democracy, reconciliation and reconstruction.[31] When people cannot trust the sources of information, it is impossible for communities to build a shared understanding of facts and without that understanding, there can be no common basis for constructive exchanges to enable mediation and reconciliation. In protracted and frozen conflict situations such as Nagorno-Karabakh[32] or the State of Palestine,[33] disinformation, propaganda and distorted narratives from various parties in the conflict area and outside have hindered conflict resolution and peace processes for decades.

C. Vectors of manipulated information

27. Disinformation, propaganda and hate speech are not peculiar to armed conflicts. They are used also at other times and spread in an amorphous way across the various phases and cycles of tensions and unrest that precede or follow armed conflicts. The underlying causes of conflict, namely, historic grievances, systemic inequalities, discrimination, intercommunal and ethnic rivalry, political tensions and poor governance, provide a perfect breeding ground for them. The dynamics of division, polarization and dehumanization that characterize violence and conflicts sustain and are sustained by such manipulation of information.

28. The gamechanger for disinformation in war, as well as peace, has been digital technology. In Ethiopia, an estimated 70 per cent of disinformation has been spread by social media.[34]

29. Technological innovation makes it possible to create "deep fake" images, videos and text that convincingly distort reality, while the business models and techniques of digital and social media platforms facilitate their rapid spread at scale and speed.[35] Microtargeting techniques, algorithmic recommendations and network effects fuel information formats and content that stimulate cognitive and emotional biases ,such as surprise, anger, disgust or outrage, to gain and sustain users' attention.[36] They also accentuate echo chambers and polarize audiences along political and sectarian lines.

---

[31] See Mercy Corps, "Strengthening social cohesion for violence prevention: Ten lessons for policymakers and practitioners", March 2022, available at https://www.mercycorps.org/sites/default/files/2022-06/10-Lessons-SC-Brief_V6_EU.pdf; see also T.M. Sagherian-Dickey, "The importance of trust in achieving positive peace" in *The Palgrave Handbook of Positive Peace*, 31 July 2021, available at https://link.springer.com/referenceworkentry/10.1007/978-981-15-3877-3_52-1#citeas.

[32] See European Resources for Mediation Support, "Media and disinformation in the Nagorno-Karabakh conflict and their role in conflict resolution and peacebuilding", January 2021, available at https://www2.coleurope.eu/system/tdf/uploads/news/event_report_-_media_and_disinformation_in_the_nagorno-karabakh_conflict.pdf?&file=1&type=node&id=draft&force=.

[33] Submission of 7amleh - Arab Center for Advancement of Social Media; see also Sheera Frankel, "Lies on social media inflame Israeli-Palestinian conflict" in *The New York Times*, 14 May 2021, available at https://www.nytimes.com/2021/05/14/technology/israel-palestine-misinformation-lies-social-media.html.

[34] See European Institute of Peace, "Fake news misinformation and hate speech in Ethiopia: A vulnerability assessment", 12 April 2021, available at https://www.eip.org/wp-content/uploads/2021/04/Fake-News-Misinformation-and-Hate-Speech-in-Ethiopia.pdf.

[35] See Dan Boneh and others, "Preparing for the age of deepfakes and disinformation", Stanford University Human-Centred Artificial Intelligence, November 2020, available at https://hai.stanford.edu/sites/default/files/2020-11/HAI_Deepfakes_PolicyBrief_Nov20.pdf; see also Ben Buchanan and others, "Truth, lies and automation: How language models could change disinformation", Center for Security and Emerging Technology, May 2021, available at https://cset.georgetown.edu/wp-content/uploads/CSET-Truth-Lies-and-Automation.pdf.

[36] See Matthew Shaer, "What emotion goes viral the fastest?" in *Smithsonian Magazine*, April 2014, available at https://www.smithsonianmag.com/science-nature/what-emotion-goes-viral-fastest-180950182/.

30. Despite the increased use of social media, legacy media remain the most common source of news for most people in conflict areas. While public interest journalism is a key tool for countering manipulated information, some media outlets, especially State-controlled media, are a vector for disinformation, propaganda and hate speech.[37] There is a risk also for independent media to proliferate manipulated information if they rely on government officials as their sole source or are reluctant to question official statements.

31. It is interesting to note the interplay between online and offline settings. In Yemen, for instance, as traditional media outlets have taken sides in the conflict, young Yemenis have increasingly resorted to social media to get their news but have found themselves exposed to false news.[38] In Myanmar, increased scrutiny and content moderation by platforms have led the authorities to augment online campaigns with offline propaganda, using pamphlets, fliers, letters and local newspapers.[39] In both cases, the consequences of online hate have manifested in offline violence.

32. The growth of disinformation cannot be attributed solely to digital technology or the underlying causes of conflicts. The vectors are multiple, including State and non-State actors, political parties, armed groups and businesses supported by paid troll armies and public relations companies. In the present report, the Special Rapporteur focuses mainly on the roles and responsibilities of States and social media companies.

III. Mapping the legal landscape

A. Concurrent application of international human rights and humanitarian law

33. It is now well recognized that international human rights law and international humanitarian law apply concurrently in armed conflicts.[40] While the International Court of Justice has noted that "some rights may be exclusively matters of international humanitarian law; yet others may be exclusively matters of human rights law; yet others may be matters of both these branches of international law",[41] according to the Human Rights Committee, the two regimes are "complementary, not exclusive".[42]

34. The application of international human rights law alongside international humanitarian law is vital for the effective protection of the right to freedom of opinion and expression during conflicts. International humanitarian law is triggered only at the onset of armed conflict and is concerned primarily with the conduct of military operations and the protection of certain classes of persons in international and non-international conflicts. As such, it covers freedom of expression and access to information issues "only tenuously and non-systematically".[43] Human rights principles and standards can provide clarity and protection where international humanitarian law is silent, absent or unclear.

---

[37] Submission of Article 19.

[38] See Ark, "Fake news and disinformation in Yemen's conflict", 5 June 2021, available at https://www.ark.international/ark-blog/fake-news-and-disinformation-in-yemens-conflict.

[39] See Andrew Nachemson and Frontier Myanmar, "Military disinformation moves offline amid Internet restrictions", 28 January 2021, available at https://www.frontiermyanmar.net/en/military-disinformation-moves-offline-amid-internet-restrictions/; see also submission of Free Expression Myanmar.

[40] See International Court of Justice, Advisory opinion on the legality of the threat or use of nuclear weapons, 8 July 1996.

[41] See International Court of Justice, Advisory opinion on the legal consequences of the construction of a wall in the Occupied Palestinian Territory, 9 July 2004.

[42] CCPR/C/21/Rev.1/Add.13, para. 11.

[43] See https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20inupholdiformation%20space%20in%20times%20of%20armed%20conflict.pdf.

35. The mutually reinforcing nature of the two legal regimes offers important possibilities for upholding freedom of opinion and expression in the face of emerging and complex challenges in the digital age. For instance, international humanitarian law applies only to parties engaged in an armed conflict, whereas human rights obligations are applicable to a broader range of actors involved in the manipulation of information. Furthermore, certain types of manipulation that are permissible under international humanitarian law can be restricted under the human rights regime. The concurrent application of both regimes thus provides the scope for a calibrated approach.[44] On the other hand, international humanitarian law gives greater protection than international human rights law against certain specific threats in times of war.

B. Information manipulation under international human rights law

36. The right to freedom of opinion and expression is enshrined in article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights. Freedom of opinion is an absolute right, not subject to limitation, restriction or derogation, even during armed conflict.[45]

37. Freedom of expression includes the freedom to seek, receive and impart information and ideas of all kinds, true or false, offensive or enlightened, regardless of frontiers and in any media of one's choice. It may be restricted only through measures that are lawful and strictly necessary to protect the rights and reputations of others, national security, public order, public health or public morals.[46] The principle of legality requires that restrictions be made by laws that are clear, precise and public and do not confer undue discretion on officials. The principle of necessity requires the restriction to be proportionate and narrowly construed to achieve the legitimate aims set out in article 19 (3) of the Covenant.

38. Disinformation cannot be prohibited under international human rights law unless it amounts to advocacy of hatred that constitutes incitement to hostility, violence and discrimination. It may be restricted only if it meets the requirements of legality, necessity and legitimate objectives as set out in the Covenant. Falsity or manipulation of information is not in itself a sufficient ground for restricting freedom of expression. In most cases, the best antidote to disinformation is not legal restriction but the free flow of diverse and verifiable sources of information, including through independent, free and pluralistic media, trustworthy public information, and media and digital literacy.[47]

39. Freedom of expression protects propaganda like any other speech. It may be restricted under the same conditions as disinformation described above. Propaganda for war, however, must be prohibited.[48] The prohibition is understood to be applicable only in relation to aggression or breach of peace contrary to the Charter of the United Nations and limited to incitement of war and not to propaganda during war.[49] Interpreting "war" as aggression precludes the misuse of this provision to crush internal disturbances, while limiting it to incitement of aggression allows States that have been attacked to rally support in self-defence. There is, however, confusion

[44] See Eian Katz, "Liar's war".
[45] CCPR/C/GC/34.
[46] Article 19 (3) of the International Covenant on Civil and Political Rights.
[47] A/HRC/47/25 and A/HRC/49/L.31/Rev.1.
[48] Article 20 (1) of the International Covenant on Civil and Political Rights.
[49] See Andrei Richter, "The Relationship between Freedom of Expression and the Ban on Propaganda for War in *European Yearbook on Human Rights 2015*; see also submission of Article 19.

among some States and companies about its scope, which underlines the need for further clarification.[50]

40. Advocacy of hatred that constitutes incitement to hostility, violence and discrimination is prohibited under international law, but States are not required to criminalize it. The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, endorsed by the Human Rights Council, provides guidance on assessing the appropriateness of criminalization in the light of six factors, including the social context, the speaker's status and intent, the content and form of the speech, the nature of the audience, the reach of the communication and the imminence of harm.[51] The guidelines are equally applicable to conflicts as to other settings.

41. Incitement to discrimination, hostility and violence is also prohibited by the International Convention on the Elimination of All Forms of Racial Discrimination, with criminalization required only in "serious cases".[52]

42. International law allows States to derogate from certain rights, including freedom of expression, during an emergency "which threatens the life of the nation".[53] While derogation gives a State greater licence to restrict expression, it does not mean that the right can be suspended without limits. Measures under derogation must be time-limited, proportionate and only "to the extent strictly required by the exigencies of the situation". They should not be discriminatory or inconsistent with the State's other international obligations or violate the peremptory norms of international law. Furthermore, derogation does not allow any action to be taken that is "aimed at the destruction" of the right itself.[54] Thus, even under derogation, the right to freedom of expression enjoys a degree of protection.

43. Manipulation of freedom of opinion deserves more attention from States and social media companies in the light of its gravity. Freedom of opinion enjoys absolute protection under international human rights law, whether in war or peace. Coercive, involuntary or non-consensual manipulation of the thinking process, such as indoctrination or "brainwashing" by State or non-State actors, violates freedom of opinion. Content curation through powerful platform recommendations or microtargeting, which plays a key element in amplifying disinformation and aggravating political tensions, is non-consensual manipulation of users' innermost thinking processes in digitized form. As such, it amounts to a violation of the right to freedom of opinion.[55]

C. Information manipulation under international humanitarian law

44. International humanitarian law has been described as taking "a remarkably lenient approach" to information manipulation during armed conflict.[56] Disinformation campaigns including ruses or the manipulation of information in order to undermine the adversary's will to resist, subterfuge and other forms of deception and propaganda are widely used by belligerents and are not unlawful under international humanitarian law.

---

[50] Submissions of Centre for Law and Democracy and Meta.
[51] A/HRC/22/17/Add.4, appendix.
[52] Article 4.
[53] Article 4 of the International Covenant on Civil and Political Rights.
[54] Article 5 (1) of the International Covenant on Civil and Political Rights.
[55] See Evelyn Aswad, "Losing the freedom to be human" in *Columbia Human Rights Law Review*, 29 February 2020). See also A/HRC/47/25, paras. 33–36.
[56] See Eian Katz, "Liar's war".

45. There are some limitations to manipulation of information under international humanitarian law.[57] Perfidy (misleading acts designed to induce one side to extend protections of international humanitarian law to the adversary so that it can kill, injure or capture) is prohibited. Certain harmful consequences arising from information operations are also prohibited, such as threats of violence or attacks to spread terror among civilian populations, encouragement of violations of international humanitarian law or incitement to commit war crimes, and threats or orders that no quarter be given or that civilians be attacked. All forms of inhumane treatment, outrages against personal dignity or humiliating or degrading treatment are prohibited against persons who are not participating in hostilities.[58] These rules apply to actions taken through any means, including as part of incitement, disinformation and propaganda campaigns on media or social media.

46. Some experts have questioned whether these limitations are adequate in the light of the nature and impact of disinformation campaigns using digital technology and social media that are directed at civilians rather than the military.[59] This is a valid concern that deserves serious consideration from United Nations treaty bodies, States and international organizations.

D. Protection of journalists

47. Uncensored and unhindered news media and the right of journalists[60] to work safely and without fear are not only integral to the right to freedom of opinion and expression, but also key to countering disinformation, including in conflict settings. International human rights law protects the practice of free, independent and pluralistic journalism and the right of journalists to free expression,[61] while international humanitarian law is silent on the issue.

48. International humanitarian law protects journalists as civilians. The deliberate killing of a journalist is a war crime.[62] The dissemination of propaganda by journalists, even though such activity supports a war effort, does not legitimize the targeting of journalists or media facilities.[63] Journalists or media outlets may become a legitimate military objective if they participate directly in hostilities or incite war crimes or other international crimes.[64]

---

[57] See Robin Geiss and Henning Lahmann, "Protecting the global information space in times of armed conflict, Geneva Academy, February 2021, available at https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20the%20Global%20information%20space%20in%20times%20of%20armed%20conflict.pdf. See also Dapo Akande, "Oxford statement on international law protections in cyberspace: The regulation of information operations and activities", Just Security, 2 June 2021, available at https://www.justsecurity.org/76742/oxford-statement-on-international-law-protections-in-the-regulation-of-information-operations-and-activities/.

[58] Geneva Conventions of 12 August 1949, common article 3.

[59] See Geiss and Lahmann, "Protecting the global information space" and Eian Katz, "Liar's war".

[60] The term "journalist" includes professional journalists, analysts, media workers, bloggers and others engaged in journalism: see A/HRC/50/29, paras. 15–16.

[61] A/HRC/50/29.

[62] Article 8 (2) (a), Rome Statute of the International Criminal Court.

[63] See Nils Melzer, *Interpretative guidance on the notion of direct participation in hostilities under international humanitarian law* (ICRC, Geneva, May 2009), available at https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf, See also submission of The Centre for Law and Democracy.

[64] See International Criminal Tribunal for the Former Yugoslavia, Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against the Federal Republic of Yugoslavia, available at https://www.icty.org/en/press/final-report-prosecutor-committee-established-review-nato-bombing-campaign-against-federal.

49. The challenge for the protection and safety of journalists in conflict settings is not one of legal gaps but the lack of political will and the failure of States and other parties to the conflict to comply with international law.

E. Extraterritorial responsibility for human rights

50. Digital technology has made it possible for information to be manipulated remotely and to impact human rights from across borders. However, extraterritorial application of international human rights law is a complex and controversial issue, raising concerns of sovereignty and security as well as human rights. Neither international human rights law nor international humanitarian law appear to have a clear answer to the thorny question of what are the responsibilities of States that inject, spread or sponsor propaganda, disinformation or incitement from across borders in conflicts to which they are not a party.

51. Under article 2 (1) of the International Covenant on Civil and Political Rights, States parties are required to respect and ensure the rights in the Covenant to all individuals within their territory and subject to their jurisdiction. That provision has been interpreted by the Human Rights Committee to include both those who are in the territory and those who are outside the territory but within the effective control of the State concerned.[65] On the other hand, the Human Rights Committee has also taken the position, in a case relating to transfer of physical custody, that a State may be responsible for extraterritorial violation of human rights if it is a link in the causal chain that made the violation possible.[66]

52. This decision suggests that the power of effective control should be considered not only over the person or the territory where they are located but over their human rights. Such an approach offers a possible route to accountability in situations where human rights violations are committed remotely using digital technology.[67]

IV. State responses: concerns, challenges and good practices

53. The General Assembly and the Human Rights Council have affirmed that responses to disinformation must be grounded in human rights.[68] State responses range from policies and practices that promote the free flow of information in line with international human rights law to actions that seek to fight disinformation using measures that undermine human rights and to some situations in which the State itself is implicated in making, sponsoring and spreading disinformation, propaganda and hate speech.

A. Promoting access to information

54. There are many examples of good practice by States to counter disinformation through measures that improve access to diverse and verifiable sources of information. These include robust laws and policies on access to information, transparency of governance, factual trustworthy public information and the promotion of independent, free, plural and diverse media.[69]

---

[65] CCPR/C//21/Rev.1/Add.13, para. 10.
[66] CCPR/96/D/1539/2006.
[67] See Ido Kilovaty, "An Extraterritorial Human Right to Cybersecurity" in *Notre Dame Journal of International and Comparative Law*, vol. 10, No. 1.
[68] General Assembly resolution 76/227 and A/HRC/49/L.31/Rev.1.
[69] A/HRC/50/29.

55. A number of Governments, in particular those of Denmark, Finland, Norway and Sweden, have invested significantly in digital, media and information literacy to build social resilience against disinformation.[70]

56. At the level of the European Union, various legislative and policy measures have been launched to support member States in addressing the threats of disinformation, including the European Democracy Action Plan, the strengthened Code of Practice on Disinformation and a co-regulatory framework under the Digital Services Act. The European Union is also funding programmes to support civil society initiatives against disinformation, such as media and fact-checking projects.[71]

57. There are various initiatives to support crisis response. One example is visa arrangements for the evacuation of independent journalists and human rights defenders from conflict-affected or repressive situations so that they can continue reporting, monitoring and fact-checking from abroad.

B. State-sponsored disinformation and propaganda

58. To some extent, all States, regardless of their political or ideological hue, produce and distribute propaganda. As noted above, State propaganda is not per se unlawful under international law. Concerns arise with propaganda for war or when the State uses false information in a way that people cannot distinguish facts from falsehood and that is likely to cause social harm or violate human rights. Under certain circumstances, State-sponsored propaganda or disinformation can amount to incitement of war crimes, as happened in Myanmar.[72]

59. State-led or sponsored disinformation has a potent impact on human rights, the rule of law, democratic processes, national sovereignty and geopolitical stability because of the resources and reach of States and because of their ability to simultaneously suppress independent and critical voices in the country so that there can be no challenge to the official narratives.[73] In a joint statement, the Special Rapporteur and equivalent mandate holders of regional organizations expressed their serious concern at the disinformation regarding the conflict in Ukraine in Russian State-owned media as well as the erosion of freedom of expression in the Russian Federation and the further tightening of media censorship, blocking of pluralist sources of information and suppression of critical voices in the wake of the Russian invasion of Ukraine.[74]

60. Digital technology has made it easier for some States and their agents, as well as non-State actors, to interfere in conflicts from across borders and spread disinformation in ways that make attribution and accountability problematic.

---

[70] See Michael Forsman, “Media literacy and the emerging media citizen in the Nordic media welfare State” in *Nordic Journal of Media Studies*, 6 June 2020, available at https://www.sciendo.com/article/10.2478/njms-2020-0006.

[71] Submission of the European Union.

[72] A/HRC/39/CRP.2; see also submission of Free Expression Myanmar.

[73] The Democratic People’s Republic of Korea is an extreme example of “ubiquitous” propaganda, tightly controlled State media and no independent or external media. See A/HRC/25/CRP.1, paras. 187 and 197–221.

[74] See African Commission on Human and Peoples’ Rights, Inter-American Commission for Human Rights and Organization for Security and Cooperation in Europe, Joint statement on the situation in Ukraine, 3 May 2022, available at https://srfreedex.org/joint-statement-on-the-situation-in-ukraine/; see also joint submission of Memorial Human Rights Defence Centre, Mass Media Defence Centre, Net Freedoms Project and OVD-Info.

Allegations of such "information operations" have been reported and hotly contested in conflicts in, for example, Libya, Mali, the Syrian Arab Republic and Yemen.[75]

C. Attacks on media and human rights defenders

61. By fact-checking and providing diverse, verifiable information, independent, free and pluralistic media play a key role in countering disinformation and State propaganda. That is why it is worrying that the media have come under severe pressure in many conflict-affected or neighbouring countries. Measures include the expulsion of foreign media, the closure of local news outlets, prosecution under "false news" or national security laws that contravene international legal standards, and attacks against journalists.

62. Mali banned French media channels for spreading "false allegations" of human rights abuses by the army.[76] Kyrgyzstan prosecuted a national independent media outlet for war propaganda because it disseminated an article on the border conflict with Tajikistan that did not match the official version.[77] Digital activism was key to exposing abuses in the Syrian war. Earlier in 2022, the Syrian Arab Republic criminalized "fake news … that undermines the prestige of the State or prejudices national unity" and arrested people for communicating with social media sites outside the country.[78] The Russian Federation adopted a law making it a serious criminal offence to publish any news about the war in Ukraine that differed from the official version. The total information blackout forced independent Russian outlets to suspend their activities or close down and Western media to leave or be blocked from reporting by the Russian authorities.[79]

63. National security and counter-terrorism laws are often used to silence critical voices, including journalists, human rights defenders and political opponents. Many of those laws fail to meet the three-pronged test of legality, necessity and legitimate aims set out in article 19 (3) of the International Covenant on Civil and Political Rights. For instance, Myanmar's military Government has expanded its criminal law to include not only "false news" but new national security provisions that criminalize causing "hatred, disobedience or disloyalty towards the military and Government".[80]

64. The banning of a media outlet is a severe restriction of freedom of expression and rarely justified. The European Commission banned several Russian State-owned media outlets on the ground that they constituted a threat to public order and security by spreading disinformation and propaganda. The necessity and proportionality of the

---

[75] See Léa Ronzaud, Ira Hubert and Ben Nimmo "Capture the flag: Iranian operators impersonate anti-Netanyahu 'black flag' protestors, amplify Iranian narratives", Graphika, 6 November 2020, available at https://graphika.com/reports/capture-the-flag; Africa Center for Strategic Studies, "A light in Libya's fog of disinformation", 9 October 2020, available at https://africacenter.org/spotlight/light-libya-fog-disinformation/; Graphika and The Stanford Internet Observatory, "More Troll-Kombat: French and Russian influence operations go head to head targeting audiences in Africa", 2020, available at https://graphika.com/reports/more-troll-kombat; and Institute for Strategic Dialogue, "Digital investigation on Syria's disinformation" in *Deadly Disinformation: How Online Conspiracies about Syria Cause Real-World Harm* (13 July 2022), available at https://www.isdglobal.org/digital_dispatches/isds-digital-investigation-on-syria-disinformation/.

[76] OHCHR, statement on "Concerns for independent media in Mali after shutdowns", 29 April 2022, available at https://www.ohchr.org/en/press-briefing-notes/2022/04/concerns-independent-media-mali-after-shutdowns.

[77] Submission of IFEX.

[78] See Mark Frary, "Syria passes draconian cybercrime laws" in *Index on Censorship*, 6 May 2022, available at https://www.indexoncensorship.org/2022/05/syria-passes-draconian-cybercrime-laws/.

[79] OHCHR press briefing on "Russia: UN experts alarmed by 'choking' information clampdown", 12 March 2022, available at https://www.ohchr.org/en/press-releases/2022/03/russia-un-experts-alarmed-choking-information-clampdown.

[80] See Shawn W. Crispin, "Bitter reversal: Myanmar military coup wipes out press freedom gains", Committee to Protect Journalists, 28 July 2021, available at https://cpj.org/reports/2021/07/bitter-reversal-myanmar-journalists-jailed-imprisoned-military-crackdown/.

ban has been questioned in a region where independent media and fact-checkers are able to challenge disinformation and where other less drastic measures could have been considered.[81]

65. Journalists reporting from the frontlines play a critical role in debunking false information but are themselves at high risk of intimidation, harassment, abduction, violence and being killed for doing their job. The Security Council has condemned attacks against journalists and media workers and has called upon all parties to end such practices.[82]

66. Targeted killing of a journalist is a war crime under international law, and yet, in 9 out of 10 cases, impunity prevails because of the lack of political will of States to investigate and prosecute.[83] A recent case in point is that of Shireen Abu Akleh, a veteran Palestinian-American journalist who was shot dead on 11 May 2022 while covering an operation by the Israeli security forces in the occupied Palestinian Territory. Despite numerous calls, including from the special procedures, the High Commissioner for Human Rights and the Secretary-General, Israel has failed to open a criminal investigation or support an independent inquiry.[84]

D. Social media regulation

67. A number of States have enacted laws regarding intermediary liability and online content regulation that impose overly broad obligations on social media companies to monitor and remove user-generated content, including disinformation.[85] For instance, China exerts comprehensive content control over social media, banning many foreign platforms, criticism of the Government, the Communist Party and religious or social issues deemed undesirable, licensing online bloggers and influencers, and most recently, proposing that platforms must review all comments on content before publishing them.[86]

68. Severe regulation of social media has been used to restrict expression relating to armed conflicts.[87] In the Russian Federation, State authorities utilized existing as well as newly enacted regulatory measures to rapidly control information on the war in Ukraine.[88] Meta reported that the authorities had issued takedown requests for war-related content posted to Facebook, with which Meta did not comply.[89] Authorities ultimately blocked Facebook and Instagram, as well as Twitter, in March 2022.[90] In addition, Google's subsidiary in the Russian Federation filed for bankruptcy after its Russian bank account was frozen, reportedly in connection with banned content on

[81] A/HRC/50/29, para 62. However, the European Court of Justice upheld the broadcast ban: See *RT France v. Council*, available at https://curia.europa.eu/juris/documents.jsf?num=T-125/22.
[82] Security Council resolution 2222 (2015).
[83] United Nations Educational, Scientific and Cultural Organization concept on "Countering threats of violence and crimes against journalists to protect freedom of expression for all", 2 November 2021, available at https://en.unesco.org/sites/default/files/concept_note_-_idei_2021_en.pdf.
[84] Communication AL ISR14/2022.
[85] A/HRC/38/35, sect. III.A, and A/HRC/47/25, paras. 56–58.
[86] See https://freedomhouse.org/country/china/freedom-net/2021; see also Zeyi Yang, "Now China wants to censor online comments" in *MIT Technology Review*, 18 June 2022, available at https://www.technologyreview.com/2022/06/18/1054452/china-censors-social-media-comments/.
[87] Communication OL RUS 4/2019.
[88] Joint submission of Mass Media Defence Centre, Memorial Human Rights Defence Centre, Net Freedoms Project and OVD-Info and submission of Access Now.
[89] Submission of Meta.
[90] Joint submission of Mass Media Defence Centre, Memorial Human Rights Defence Centre, Net Freedoms Project and OVD-Info.

its services, data localization requirements, and the restrictions that Google applied to Russian media outlets' YouTube channels.[91]

69. States should not require platforms to enforce regulations that do not conform with international human rights law. Whether during conflicts or in other settings, the Special Rapporteur has recommended "smart regulation" of Internet intermediaries to ensure their compliance with human rights due diligence, meaningful transparency and due process requirements, rather than viewpoint- or content-based regulation.[92]

E. Disruptions to the Internet and telecommunications

70. The Human Rights Council has condemned Internet shutdowns unequivocally and urged States to refrain from them.[93] Shutting or slowing down this vital means of communications aggravates rather than combats disinformation, propaganda or incitement.

71. Access to the Internet is vital, especially in conflict-affected contexts where it may be the only avenue of communication with the external world. Internet shutdowns have been frequent in countries suffering from conflict, including Ethiopia, Myanmar, the Sudan and the Syrian Arab Republic, as a means for Governments to control the flow of information.[94] The impact of the shutdowns and "throttling" or slowdowns can be devastating on people's everyday lives. The disruptions also inhibit monitoring and reporting by human rights defenders and journalists. Correlations between shutdowns and abuses associated with military movements, demonstrations and coups are troubling.[95]

72. Under international humanitarian law, media facilities are civilian objects, even if they are disseminating propaganda in support of the war. They must not be targeted unless they are being used directly in hostilities. Nevertheless, telecommunications infrastructure or premises of media outlets have been bombed or shelled during conflict, including in Ukraine, Yemen and the Gaza Strip.[96]

73. Overly broad sanctions by States and overzealous compliance by companies can interfere with online access and flow of information in sanctioned and sanctioning countries. The sanctions can be counterproductive by making it more difficult for the public, civil society and human rights defenders in these countries to access diverse sources of information, as has happened in the Islamic Republic of Iran, the Russian Federation, the Sudan and the Syrian Arab Republic, or for those elsewhere to know what is happening in the countries.[97]

---

[91] See Interfax, "Russian subsidiary of Google files for bankruptcy", 17 June 2022, available at https://interfax.com/newsroom/top-stories/80331/.

[92] A/HRC/47/25, para. 91.

[93] A/HRC/47/L.22, para. 11.

[94] See #KeepItOn, "The return of digital authoritarianism: Internet shutdowns in 2021", April 2022, available at https://www.accessnow.org/cms/assets/uploads/2022/05/2021-KIO-Report-May-24-2022.pdf.

[95] A/HRC/50/55, para. 27; see also submission of Access Now.

[96] Submission of Access Now.

[97] Ibid.

V. Social media companies: roles and responsibilities

A. Social media in conflict settings

74. Social media platforms are highly susceptible to the spread of disinformation, propaganda and incitement given their reliance on algorithms to target users with particular content and recommendations, based in part on data collected about those users. Numerous reports from civil society, the media, researchers and international organizations have pointed to the role of social media in spreading State propaganda, extremist content and disinformation in Ethiopia,[98] Myanmar,[99] Ukraine[100] and Yemen.[101]

75. Among social media companies, Meta has drawn the most attention as a result of Facebook's role in amplifying hatred and violence in countries such as Myanmar, where the independent international fact-finding mission appointed by the Human Rights Council declared Facebook to be "the leading platform for hate speech".[102] In the war in Ukraine, Meta set up a special operations centre with Russian and Ukrainian speakers and is working with local and international partners and fact-checkers to address information manipulation, but it has also deployed a singular "expression of self-defence" exception to its hate speech policies, which permits Ukrainian users to express resistance and fury against the Russian military.[103]

76. Information manipulation is also prevalent on other platforms. One study found that YouTube had served as a heavily monetized, foundational source for cross-platform spread of disinformation and extremist content.[104] Twitter has faced criticism with respect to its role in a number of conflicts.[105] Content concerning the war in Ukraine, including disinformation, has increased significantly on TikTok.[106] Weibo similarly noted a rise in content inaccurately represented as originating from Ukraine and announced that it would enforce the automatic addition of geolocation to posts concerning the conflict.[107] Telegram, which has a hands-off approach to restrictions on expression, is used extensively in the Russian Federation and Ukraine

---

[98] Submission of the Oversight Board (Raya Kobo case); see also Global Witness, "Now is the time to kill".

[99] Submission of Free Expression Myanmar.

[100] Joint submission of Mass Media Defence Centre, Memorial Human Rights Defence Centre, Net Freedoms Project and OVD-Info; see also Carl Miller "Who's behind #IStandWithPutin?" in *The Atlantic*, 5 April 2022, available at https://www.theatlantic.com/ideas/archive/2022/04/russian-propaganda-zelensky-information-war/629475/.

[101] See Hannah Porter, "A conversation on fighting disinformation in Yemen", Yemen Policy Center, March 2022, available at https://www.yemenpolicy.org/a-conversation-on-fighting-disinformation-in-yemen/.

[102] A/HRC/42/50, para. 72.

[103] See Meta, "Meta's ongoing efforts regarding Russia's invasion of Ukraine", 26 February 2022, available at https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/.

[104] See Paul M. Barrett and Justin Hendrix, "A platform 'weaponized': How YouTube spreads harmful content – and what can be done about it", Stern Center for Business and Human Rights, June 2022, available at https://static1.squarespace.com/static/5b6df958f8370af3217d4178/t/62a38fc022745a7274601da0/1654886337000/NYU+CBHR+YouTube_Final_June10.pdf.

[105] See Torinmo Salau, "How Twitter failed Africa", Foreign Policy, 19 January 2022, available at https://foreignpolicy.com/2022/01/19/twitter-africa-ghana-dorsey-disinformation/.

[106] See Sara Brown, "In Russia-Ukraine war, social media stokes ingenuity, disinformation", MIT Sloan School of Management, 6 April 2022, available at https://mitsloan.mit.edu/ideas-made-to-matter/russia-ukraine-war-social-media-stokes-ingenuity-disinformation.

[107] See Weilun Soon, "How China's tech giants, from TikTok to Tencent, are reacting to Russia's invasion of Ukraine", Insider, 13 April 2022, available at https://www.businessinsider.com/how-chinas-tech-giants-reacting-to-ukraine-crisis-tiktok-tencent-2022-3?r=US&IR=T.

by both the authorities and the public to circulate information regarding the conflict, including disinformation and propaganda.[108]

77. As the above-mentioned examples illustrate, the use of social media to amplify manipulated information in conflicts is widespread and growing. Companies need to ramp up action to prevent incitement to violence and other serious human rights violations while ensuring respect for freedom of opinion and expression.

B. Corporate legal standards during conflicts

78. International human rights law and international humanitarian law are both applicable to companies in situations of armed conflicts. As stated in the Guiding Principles on Business and Human Rights,[109] companies have a responsibility to respect internationally recognized human rights and to conduct their operations in ways that avoid causing or contributing to "adverse human rights impacts" and to prevent or mitigate such impact; adopt policies reflecting their commitment to respect human rights; carry out human rights due diligence; and provide processes for remediation of adverse human rights impacts they cause or to which they contribute.

79. Social media or telecommunications companies that provide the means to distribute information in a conflict setting may be sufficiently linked to armed conflict to trigger the application of international humanitarian law to their operations. Company personnel may be held liable for serious violations of international humanitarian law amounting to war crimes,[110] either on the basis of direct action or corporate complicity.[111] Moreover, they may lose their protection as civilians under international humanitarian law if they engage in activity that could be construed as direct participation in hostilities.[112] In such situations, companies have a dual responsibility: first, to continue to respect freedom of opinion and expression, including the right to information, and second, to comply with international humanitarian law.

80. The Working Group on business and human rights has called on companies operating in conflict situations (including pre- and post-conflict) to exercise heightened due diligence in line with the heightened risks.[113] The United Nations has identified "increased inflammatory rhetoric or hate speech targeting specific groups or individuals" as a "red flag" that should prompt companies to initiate heightened due diligence.[114] It has advised companies to identify and assess their actual or potential adverse impacts not only on human rights, but also on the conflict itself.

81. Civil society organizations have emphasized the importance of synthesizing human rights, conflict sensitivity, technology ethics and human security frameworks in order to develop effective approaches for digital company operations in conflict

---

[108] See Sara Brown, "In Russia-Ukraine war".

[109] A/HRC/17/31, annex.

[110] See Guiding Principles on Business and Human Rights, commentary on principle 23; OHCHR, *The Corporate Responsibility to Respect Human Rights: An Interpretive Guide*, 2012, available at https://www.ohchr.org/sites/default/files/Documents/Publications/HR.PUB.12.2_En.pdf; and ICRC, IHL database, available at https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule156.

[111] A/HRC/50/40/Add.4, para. 34.

[112] See Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, article 51 (3) and OHCHR, *The Corporate Responsibility to Respect Human Rights*.

[113] A/75/212, paras. 13, 19–21 and 72; see also Guiding Principles on Business and Human Rights, principles 7 and 17.

[114] See Gerald Pachoud and Siniša Milatović, "Heightened Human Rights Due Diligence for Business in Conflict-affected Contexts: A Guide", United Nations Development Programme, 2022, available at https://www.undp.org/sites/g/files/zskgke326/files/2022-06/UNDP_Heightened_Human_Rights_Due_Diligence_for_Business_in_Conflict-Affected_Context.pdf.

settings. They have also proposed that a model framework based on this approach be developed through a multi-stakeholder process.[115]

C. Company policies

82. The war between Ukraine and the Russian Federation and the actions by the Russian Federation to criminalize independent war reporting and ban media outlets jolted social media companies into an unprecedented level of action.[116]

83. Almost all Western companies have left the Russian Federation or have been blocked. Some companies based in the United States of America have made widely reported announcements regarding their efforts to maintain Internet access in Ukraine and resist censorship and propaganda in the Russian Federation. Much less is known about their responses in conflicts in other parts of the world or about the policies and practices of companies headquartered outside Western Europe and North America. Not surprisingly, there are concerns about the consistency of companies' policies globally and the depth of their commitment to human rights.

84. The published policies of companies on conflict and manipulation of information vary widely, with some continuing to evolve in response to developments on the ground. For example, Twitter has issued an official "crisis misinformation policy", in which it is stated that the company "will take action on accounts that use Twitter's services to share false or misleading information that could bring harm to crisis-affected populations".[117] Meta has developed procedures for handling "countries at risk", which it has detailed in public posts,[118] and is reported to be working on a conflict policy after disinviting its Oversight Board from advising on content moderation in conflict, citing safety issues.[119] Other platforms, including Reddit, Snapchat and TikTok, have so far only opted to issue statements addressing concerns specific to particular conflict situations.[120]

85. As noted by the previous mandate holder and reiterated by the present Special Rapporteur, companies should incorporate human rights standards as a default into their terms of service, content moderation policies, rule-making and enforcement.[121]

---

[115] See Jennifer Easterday, Hana Ivanhoe and Lisa Schirch, "Comparing guidance for tech companies in fragile and conflict-affected situations", Policy Brief No. 125, Toda Peace Institute, March 2022, available at https://toda.org/policy-briefs-and-resources/policy-briefs/comparing-guidance-for-tech-companies-in-fragile-and-conflict-affected-situations.html.

[116] Telecom companies have also taken remarkable steps to maintain infrastructure in conflict-affected areas in Ukraine and provide refugees with free communication tools, and cloud services have kept access available to users.

[117] Crisis information policy, Help Center, May 2022, available at https://help.twitter.com/en/rules-and-policies/crisis-misinformation.

[118] Submission of Meta.

[119] See Meta, "Meta withdraws a policy advisory opinion request related to Russia's invasion of Ukraine", 13 July 2022, available at https://transparency.fb.com/oversight/oversight-board-cases/ukraine-russia-pao; see also Oversight Board, "Protecting freedom of expression and human rights in Ukraine and Russia", May 2022, available at https://oversightboard.com/news/382264103827624-protecting-freedom-of-expression-and-human-rights-in-ukraine-and-russia/.

[120] See Upvoted, "Supporting Ukraine and our community", 2 March 2022, available at https://www.redditinc.com/blog/supporting-ukraine-and-our-community; Team Snap, "We Support Ukraine", 1 March 2022, available at https://newsroom.snap.com/we-support-ukraine/; and TikTok, "Bringing more context to content on TikTok", 4 March 2022, available at https://newsroom.tiktok.com/en-us/bringing-more-context-to-content-on-tiktok.

[121] A/HRC/38/35; A/HRC/47/25, sect. V.

However, with a few exceptions,[122] companies seldom reference international human rights standards as a basis for their policies. Instead, they draw on their own numerous separate policies to craft responses to conflict-based challenges.[123] This fragmented approach fails to provide much-needed coherence and predictability to platform practice and has the potential to undermine company compliance with international human rights law and international humanitarian law.

D. Company practices

86. Many of the problems identified below have been raised by the previous and current Special Rapporteurs and other stakeholders in relation to non-conflict situations. They are of added significance in conflict settings because of the higher risks to companies and greater vulnerability of users. While there have been efforts to improve crisis response and content moderation, major concerns, including about the business model itself, remain largely unaddressed.

87. **Human rights due diligence**. While details on the conflict-related due diligence carried out by companies are limited, there seems to be a mismatch between the allocation of resources and the seriousness of the problems,[124] and a lack of timeliness in carrying out heightened due diligence. There is concern among civil society as to whether companies have put in place adequate processes to identify a particular operational context as presenting a potential risk of conflict.[125] Since the outbreak of the war in Ukraine in February, several companies have created or reinforced conflict teams and are working on conflict-related policies and procedures, but concrete information on how they operate and what resources are being applied are sparse. Nor is it clear whether similar structures are being created for global application.

88. **Content moderation**. In conflict situations, inadequate content moderation can fuel disinformation, propaganda and incitement and aggravate the violence. Platform users, civil society organizations and researchers report inconsistencies as well as serious failures in content moderation.

89. Reports indicate that companies have difficulty calibrating content removal in conflict settings, over-censoring in some situations while providing insufficient attention or displaying bias in some others.[126] Civil society organizations have also complained that companies are susceptible to pressure from States asking for removal of content representing dissenting viewpoints in conflict situations.[127]

90. There is concern that companies have not allocated sufficient resources and expertise to review content in all relevant languages and with an understanding of local

---

[122] Meta has noted the applicability of the Guiding Principles on Business and Human Rights, international human rights law and international humanitarian law. See submission of Meta. See also Meta, "Facebook Community Standards", available at https://transparency.fb.com/policies/community-standards/, and Meta, "Corporate Human Rights Policy", available at https://about.fb.com/wp-content/uploads/2021/03/Facebooks-Corporate-Human-Rights-Policy.pdf. Twitter has noted the applicability of international humanitarian law. See Sinéad McSweeney, "Our ongoing approach to the war in Ukraine", 16 March 2022, available at https://blog.twitter.com/en_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine.

[123] See submission of Meta.

[124] A/HRC/47/25, paras. 74–76.

[125] Submissions of JustPeace Labs and Article 19.

[126] Submissions of Access Now, Article 19 and the Oversight Board.

[127] Submissions of 7amleh Arab Center for Advancement of Social Media and the Oversight Board; see also Access Now, "Sheikh Jarrah: Facebook and Twitter systematically silencing protests, deleting evidence", 7 May 2021, available at https://www.accessnow.org/sheikh-jarrah-facebook-and-twitter-systematically-silencing-protests-deleting-evidence/.

circumstances in conflict settings.[128] Moreover, while companies incorporate both automated and human processes for content moderation, it is unclear how those processes are balanced, how well and according to what parameters automated processes have functioned or what level of local expertise is available for human moderation.

91. In addition to removing or blocking content, social media companies have also deployed tactics aimed at mediation of conflict-related content available to their users, for example, warnings, labels, fact-checking, suggestion of other sources, or reducing distribution of content.

92. **Monetization**. Reports have documented the extensive use of disinformation, propaganda and hate speech to generate revenue on social media platforms, thereby incentivizing the continued manipulation of information.[129] Such monetization has taken place in spite of company policies that purport to limit the types of content deemed suitable for advertising.[130] Recognizing that problem, the European Commission's 2022 strengthened Code of Practice on Disinformation, which Google, Meta, Microsoft, TikTok and Twitter have signed, includes commitments dedicated to demonetization efforts.[131]

93. Some social media companies have moved to restrict the monetization of certain conflict-related content, particularly in relation to the war in Ukraine (which has been affected by the application of sanctions).[132] Research suggests, however, that companies' advertising policies are not sufficiently comprehensive or adequately enforced and are not regularly updated to reflect global conflict developments.[133] Indeed, the predominant focus of the companies on the conflict in Ukraine raises questions as to whether monetization in other conflict settings is being addressed proactively.

94. **Transparency and remedy**. Digital platforms have struggled to provide meaningful transparency whether in peaceful or conflict contexts. In 2022, Ranking Digital Rights assessed that transparency reporting of 14 of the most widely used digital platforms had fallen short in providing essential context and granular data, as well as information on human rights due diligence and the development and deployment of algorithmic and targeted-advertising systems, including those used to

---

[128] Submission of Article 19.

[129] See Karen Hao, "How Facebook and Google fund global misinformation" in *MIT Technology Review*, 20 November 2021, available at https://www.technologyreview.com/2021/11/20/1039076/facebook-google-disinformation-clickbait/.

[130] See https://support.google.com/youtube/answer/6162278?hl=en#zippy=%2Cguide-to-self-certification; Help Center, "Content monetization standards", available at https://help.twitter.com/en/rules-and-policies/content-monetization-standards; Meta business advertising policies, available at https://www.facebook.com/policies_center/ads; TikTok advertising policies, available at https://ads.tiktok.com/help/article?aid=9552; and Snap advertising policies, available at https://www.snap.com/en-US/ad-policies.

[131] European Commission, Strengthened Code of Practice on Disinformation, sect. II.

[132] See YouTube channel monetization policies, available at https://support.google.com/youtube/answer/1311392?hl=en; Meta, "Meta's ongoing efforts regarding Russia's invasion of Ukraine", 26 February 2022, available at https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/#latest; Sinéad McSweeney, "Our ongoing approach to the war in Ukraine", 16 March 2022, available at https://blog.twitter.com/en_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine; Twitter policy "State media", available at https://business.twitter.com/en/help/ads-policies/ads-content-policies/state-media.html; Snap advertising policies, sect. 3.9, available at https://www.snap.com/en-US/ad-policies; Upvoted, "Supporting Ukraine and our community", 2 March 2022, available at https://www.redditinc.com/blog/supporting-ukraine-and-our-community; and Rafael Frankel, "An update on the situation in Myanmar", Meta, 7 December 2021, available at https://about.fb.com/news/2021/02/an-update-on-myanmar/. See also submission of Meta.

[133] Submission of The Global Disinformation Index.

curate, rank or recommend content.[134] Transparency around government takedown requests, including their number, origin, target and whether the company cooperated, is also limited.

95. The Oversight Board has noted the need for greater transparency on Meta's enforcement of its content policies, broken down by country and language, as well as on government requests for content removal.[135] These issues have emerged in relation to Meta because of the company's decision to create the Oversight Board. Many other companies provide little or no information on their operations, much less a public channel of appeal and review.

96. The 2022 strengthened Code of Practice on Disinformation of the European Commission, which complements and aligns with the regulatory requirements of the Digital Services Act, includes commitments to enhance transparency, improve access by the researcher community to platform data and release more information to users on the design of recommender systems.[136] While such measures represent important progress, regularly updated transparency reporting specific to developments in at-risk or conflict-affected countries is also needed.

97. In addition, secure, straightforward access to appeals mechanisms and other lines of communication, followed by timely responses, is essential for users to contest or raise concerns regarding restrictions on expression in times of conflict, including with respect to the preservation of evidence. The strengthened Code of Practice includes a commitment to provide a transparent appeal mechanism that is timely, diligent and objective.[137]

98. **Encryption, anonymity and account security**. The use of encryption, anonymity and other privacy protocols can enhance user agency and security by preventing the collection of user data, censorship and non-consensual targeting of users with customized content.[138] At the same time, platforms utilizing encryption are being used to spread hate speech and other inflammatory content. For instance, reports suggest that in Myanmar, as content moderation on Facebook increased, disinformation, propaganda and incitement became more pronounced on Telegram, with publicly accessible pro-military channels on the platform engaging in doxing.[139] It is important for stakeholders to continue to assess methods for community moderation and reporting mechanisms on platforms that incorporate encryption that both emphasize user agency and comply with international human rights law and international humanitarian law.[140]

99. **Preservation of evidence**. Preservation of evidence of violations during conflict deserves special attention by social media platforms given the importance of

---

[134] See Afef Abrougui and others, "Key findings from the 2022 RDR big tech scorecard", Ranking Digital Rights programme at New America, available at https://rankingdigitalrights.org/mini-report/key-findings-2022/; and Svea Windwehr and Jillian C. York, "Thank you for your transparency report, here's everything that's missing", Electronic Frontier Foundation, 13 October 2020, available at https://www.eff.org/deeplinks/2020/10/thank-you-your-transparency-report-heres-everything-thats-missing.

[135] Submission of the Oversight Board.

[136] European Commission, Strengthened Practice Code on Disinformation, sect. VI, commitments 18–19.

[137] Ibid., commitment 24.

[138] See joint submission of Mass Media Defence Centre, Memorial Human Rights Defence Centre, Net Freedoms Project and OVD-Info and submission of Center for Media Engagement, University of Texas at Austin.

[139] Submissions of Free Expression Myanmar and Access Now.

[140] Submission of Center for Media Engagement, University of Texas at Austin.

such data for accountability and justice processes.[141] Reports have emerged of social media companies opting to take down conflict-related content, including evidence of war crimes, because it contravenes their policies on graphic or violent images, and erring on the side of employing the fastest route to removal, without efforts to archive the material.[142]

VI. Conclusions and recommendations

100. **The information environment has become a dangerous, expanding theatre of conflict in the digital age. State and non-State actors, enabled by new technologies and social media platforms, have weaponized information to sow confusion, feed hate, incite violence, instigate public distrust and poison the information environment. The human suffering and damage to societal structures have gone far beyond the exigencies of war.**

101. **Against this background, the Special Rapporteur draws six broad conclusions, which guide the specific recommendations for stakeholders.**

102. **First, the right to information should not be considered a legitimate target of war. It is a "survival right" on which people's lives, health, well-being, safety and security depend in times of crisis and conflict. It is a human right and a public good to be nurtured and promoted for the safety, security, dignity and freedom of people. Democratic societies cannot flourish without access to diverse sources of information. Freedom of expression, which encompasses the right to information, is the basis for public trust that helps to prevent and resolve conflicts and facilitates peace, reconciliation and development.**

103. **Second, countering disinformation is vital for safeguarding human rights and restoring public trust, but it must be done in ways that are effective, not counterproductive. Censorship of critical voices, attacks on independent media and Internet disruptions do nothing to reduce disinformation and much to erode freedom of opinion and expression and degrade the information environment. All States must be unequivocal in their commitment to uphold the right to freedom of opinion and expression, and any action they take to counter disinformation should be grounded in international human rights law.**

104. **Third, digital technology and social media have created a new paradigm that has exposed ambiguities, uncertainties and potential gaps in international legal standards that some States and non-State actors are exploiting with audacity and impunity to the detriment of human rights and humanitarian protection. The application of human rights principles alongside international humanitarian law should be reinforced so that the permissible limits of "ruses of war" are reinterpreted in a way that protects both civilians as well as the right to information that they need for their dignity and survival.**

105. **The prohibition of propaganda for war should be interpreted narrowly to ensure that it does not infringe on the right to protest and criticize. Guidelines should be produced by the Office of the United Nations High Commissioner for Human Rights for the use of States and companies.**

---

[141] See Human Rights Center, University of California at Berkeley School of Law, and OHCHR, *Berkeley Protocol on Digital Open Source Investigations: A Practical Guide on the Effective Use of Digital Open Source Information in Investigating Violations of International Criminal, Human Rights and Humanitarian Law* (United Nations publication, 2022), available at https://www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.

[142] See submission of the Oversight Board.

106. **The issue of extraterritorial application of human rights should be revisited to take account of the digital threats to the right to freedom of expression and information from across borders.**

107. **Fourth, while the response of social media companies to the war in Ukraine has been commendable in many ways, they must do much more to ensure that policies and operational practices are applied consistently across the world and that enhanced human rights due diligence and impact assessment are timely and attuned to local contexts for all conflict settings in which the companies operate.**

108. **Fifth, it is essential to build social resilience against information manipulation by empowering rights holders and civil society. More attention should be given in fragile situations to media information and digital literacy, particularly for young people, women, the elderly and other marginalized groups, healthy community relations, community-based fact-checking, and education programmes to counter hatred, violence and extremism.**

109. **Lastly, the challenges of the digital ecosystem must be tackled in an integrated way, with the collaboration of all stakeholders. It is essential to pursue a multidimensional, multi-stakeholder approach in which civil society and legacy media are fully engaged alongside States, international organizations and digital companies.**

A. Recommendations for States

110. **The obligation to respect, protect and fulfil the right to freedom of opinion and expression places upon States the duty to ensure a healthy information environment. In line with that duty, States must refrain from making, sponsoring, encouraging or disseminating false information to degrade the information environment.**

111. **During armed conflict, States must not use, disseminate or encourage third parties to disseminate information within or across borders in ways that could result, directly or indirectly, in inflicting harm on civilians, including war crimes, crimes against humanity or other violations of international humanitarian law, or incitement of hostility, violence or discrimination under international human rights law.**

112. **States must not disrupt the Internet or telecommunications, as that is an inherently disproportionate restriction of access to information. General sanctions should avoid the effect of limiting people's access to the Internet or secure means of communication. Where necessary, States should provide exemptions to enable access to the Internet and the free flow of information to populations living under sanctions.**

113. **States should not prohibit or restrict disinformation, propaganda and "false news" or "fake news" unless they meet the requirements of legality, necessity and legitimate aim as set out in article 19 (3) or amount to incitement in line with article 20 of the International Covenant on Civil and Political Rights. They must prohibit advocacy of hatred that constitutes incitement to discrimination, hostility or violence, or other international crimes. Criminalization of expression should be avoided except in line with the guidance provided in the Rabat Plan of Action.**

114. **States must ensure that all derogation measures are strictly necessary and proportionate to meet exceptional situations, non-discriminatory, time-limited and tailored in scope to the exigencies of the crisis. Furthermore, the measures to restrict expression during emergencies should be declared as derogation under**

the International Covenant on Civil and Political Rights procedure to allow scrutiny by the Human Rights Committee.

115. **States should prioritize non-legal measures of countering disinformation and propaganda, starting with their own obligation to proactively disclose official data, encourage trustworthy fact-checking, promote access to diverse, reliable sources of information, ensure media, digital and information literacy and foster an enabling and inclusive environment for civil society to take initiatives to counter information manipulation.**

116. **States should fulfil their duty to ensure the right to information by increasing their own transparency and by proactively disclosing official data online and offline. All States must adopt and implement comprehensive laws on access to information or bring existing law, policies and practices into line with international and regional standards. Such laws should avoid unduly broad exceptions to the right to information on grounds of national security.**

117. **The right to information includes access to information of all kinds, regardless of borders and through any medium of the person's choice. States should respect and protect the right of individuals to receive foreign news and propaganda, unless such information has been restricted in line with the international human rights standards.**

118. **States should respect, protect and promote the independence, freedom, pluralism and diversity, including gender diversity, of the media at all times. They should comply fully with their obligations under international humanitarian law to protect all foreign and national journalists (defined according to international human rights law) as civilians in armed conflict. The media's freedom of movement and freedom to report independently should be respected scrupulously.**

119. **It is not lawful for States to compel media outlets, social media platforms or civil society organizations to disseminate only information produced or approved by the authorities during armed conflicts. Total information blackouts enforced with severe criminal punishment are not justified under international law even during states of emergency.**

120. **States should investigate all attacks on journalists promptly, effectively, independently and impartially in line with the Minnesota Protocol on the Investigation of Potentially Unlawful Death. The United Nations should establish an independent international task force to support international and national efforts to prevent, investigate and prosecute attacks against journalists.**

121. **The International Criminal Court should review the persistent killings of journalists in conflict situations with a view to prosecution of war crimes where the national authorities are unwilling or unable to do so.**

122. **States should not ask platforms to enforce measures in relation to content that do not conform with international human rights standards. State regulation of social media should encourage companies to ensure meaningful transparency, human rights due diligence and due process rights for users.**

B. Recommendations for companies

123. **Companies should develop specific comprehensive policies, processes and structures for operating in conflict settings, based on international human rights law and, where applicable, international humanitarian law standards that provide predictable, consistent and effective frameworks to address**

manipulation of information, ensure user security and establish mechanisms for remedy. The policies should be made available to all users in the language in which they engage with the platform.

124. **Companies should carry out heightened human rights due diligence and trigger enhanced risk management strategies in a timely way for pre-, post- or ongoing conflicts with adequate resources, language and contextual expertise, and engagement of civil society. Due diligence processes should incorporate robust analysis of the impact of the companies' operations, products and services, including the business model itself, on conflict dynamics as well as human rights.**

125. **Companies should align content moderation to international human rights law and international humanitarian law standards, making every effort to uphold freedom of expression and access to information while preventing the dissemination of content likely to incite violence or violate other principles of international human rights law and international humanitarian law.**

126. **Companies should ensure that content moderation in conflict settings includes robust human review, incorporating expertise in relevant languages and local and regional contexts. Internal expertise should be complemented by partnerships with reliable fact-checking organizations and civil society.**

127. **End-to-end encryption must be protected as an essential facet of the enjoyment of freedom of opinion and expression. Companies should also carefully assess account security risks that are likely to affect users in conflict settings and provide enhanced security options.**

128. **Companies should not only develop but also effectively implement policies to limit and track the monetization of harmful content linked to armed conflict.**

129. **Companies should enhance transparency in conflict situations, including through regular publicly available transparency reports dedicated to specific situations. Such reports should include the granular details and context required to effectively assess the human rights impacts of company policies. Companies should facilitate the access of researchers to company data on the use of digital platforms during conflict.**

130. **Companies should securely preserve all potential evidence of war crimes or other human rights violations perpetrated during armed conflict in accordance with international evidentiary standards and develop processes to share the evidence with appropriate national or international justice bodies.**

131. **In conclusion, the Special Rapporteur reiterates the need for more research, analysis and multi-stakeholder dialogue to build consensus on concepts, policies, strategies and guidelines to address disinformation and other forms of information manipulation. As various initiatives are launched to examine these issues, the Special Rapporteur reiterates her call for a robust human rights approach and welcomes proposals from Member States, international organizations, companies and civil society on how her mandate can contribute to their efforts.**