Access Now Submission to the United Nations Special Rapporteur on Freedom of Opinion and of Expression for the UN General Assembly 78th Session Report on Freedom of Expression: the Gender Dimensions of Disinformation

14 July 2023

Introduction

Access Now welcomes this opportunity to provide relevant information to the United Nations (UN) Special Rapporteur on Freedom of Opinion and of Expression (Special Rapporteur) to inform the thematic report on freedom of expression and the gender dimensions of disinformation to be presented to the UN General Assembly at the 78th session.[1]

Access Now, a UN Economic and Social Council (ECOSOC) accredited organization, routinely engages with the UN in support of our mission to extend and defend digital rights of people and communities at risk around the world.[2] Since its founding in 2009, Access Now monitors the abuse and misuse of new and emerging technologies that threaten fundamental human rights, including freedoms of expression, association, and peaceful assembly, as well as the rights to privacy and non-discrimination. We also closely monitor internet shutdowns and coordinate the global #KeepItOn coalition and campaign against internet shutdowns.[3]

This submission addresses gendered disinformation, including tactics of gendered surveillance and targeted harassment, and its impacts on individual rights and democracy. It is important to note that while this submission draws upon examples, these examples are non-exhaustive, and do not represent the lived experiences of all persons at risk. More information is required to take into full account the intersecting forms of oppression of those who are directly targeted.

I. Defining 'gendered disinformation': the similarities and differences between 'gendered disinformation' and online and tech-facilitated gender-based violence

1. Gendered disinformation is a subset of online abuse that aims to eliminate women and feminist opinions and expressions from public space.[4] More specifically, gendered

[1] OHCHR, Call for submissions to the thematic report of the Special Rapporteur on Freedom of Opinion and Expression to the United Nations, General Assembly, 2023, available at: https://www.ohchr.org/en/special-procedures/sr-freedom-of-opinion-and-expression.
[2] Access Now, About Us, 2021, available at https://www.accessnow.org/. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.
[3] Access Now, #KeepItOn, 2023, available at: https://www.accessnow.org/keepiton/.
[4] U.S. Department of State, Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors, 27 March 2023, available at: https://www.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors/.

disinformation weaponizes digital platforms to spread misleading and inaccurate information and stigmatize feminist stances and democratic values. Women activists, politicians, journalists, and dissidents are the main targets of gendered disinformation. Gendered disinformation exists at the intersection of online gender-based violence (GBV), disinformation, and democracy. It aims to manipulate people's political and economic choices, and also carries severe personal harms.[5]

2. Gendered disinformation is distinct from gendered misinformation and malinformation. While gendered disinformation content is intentionally false and designed to cause harm, gendered malinformation – for example, doxxing and non-consensual sharing of intimate images, or revenge porn – is "genuine information shared with the intention to cause harm."[6] Gendered misinformation is the unintentional spread of gendered disinformation.[7]

3. Tactics of gendered disinformation include, but are not limited to, targeted harassment, digital surveillance, social media monitoring, defamation, and the spread of deceptive and false information regarding women human rights defenders (WHRDs). Many of these tactics, such as digital surveillance of WHRDs, also constitute GBV. Gendered disinformation has severe individual and political impacts. On an individual level, gendered disinformation harms the mental and physical health of victims and survivors, perpetuates social isolation, and limits freedom of movement both in public and private spaces, online and offline. At a societal level, gendered disinformation deters womens' freedom of expression and undermines democracy.[8]

4. Gendered disinformation is distinct from GBV because of its political motivations, strategies of manipulation, and social effects. According to #ShePersisted, an organization working to address gendered disinformation against women in politics, "gendered disinformation deserves specific attention for its specificities and harmful impact on democracy," especially compared to the "different types of online attacks against women."[9] Overall, gendered disinformation causes a chilling effect on womens' freedom of expression, limits their democratic participation, and causes further stigmatization.

5. While all women and advocates for gender equality and women's rights may be the targets of gendered disinformation, the likelihood of attacks increases according to several factors. Some of these factors include identity, age, visibility or the level of public participation, and –

[5] Demos, Engendering Hate: The Contours of State-Aligned Gendered Disinformation Online, October 2020, 7, available at: https://demos.co.uk/wp-content/uploads/2023/02/Engendering-Hate-Oct.pdf.
[6] UN Human Rights Council Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 13 April 2021, ¶12, available at: https://eos.cartercenter.org/uploads/document_file/path/985/Report_of_the_Special_Rapporteur_on_Disinformation_and_Freedom_of_Opinion_and_Expression_E.pdf.
[7] *Ibid.*
[8] U.S. Department of State, Gendered Disinformation.
[9] #ShePersisted, Monetizing Misogyny: Gendered Disinformation and the Undermining of Women's Rights and Democracy Globally, February 2023, 7, available at: https://she-persisted.org/wp-content/uploads/2023/02/ShePersisted_MonetizingMisogyny.pdf .

for journalists and those who express themselves in media – topics they cover. For instance, "gender and women's rights, sexual violence, abortion, LGBTQ+ rights, politics and extremism are examples of hightriggering areas."[10]

6. Gendered disinformation falls under the UN definition of violence against women. The UN defines violence against women as "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.' This includes 'physical, sexual and psychological violence perpetrated or condoned by the State, wherever it occurs.'" Gendered disinformation has severe physical and psychological impacts, as evidenced by the testimonies of its victims, and thus falls under the definition of VAWG.[11]

A. Targeted Harassment: Women Politicians, Journalists, and Human Rights Defenders

7. State and non-state actors weaponize online spaces to target women politicians, journalists, and human rights defenders. Women and women's rights organizations are disproportionately attacked on social media platforms. **Globally, 73% of women journalists have been attacked online**.[12] Data from Access Now's Digital Security Helpline shows that women continue to be frequent targets of harassment, doxxing, censorship and other forms of online GBV, and that women's rights organizations face additional challenges to advance their causes and to protect themselves. Out of all cases the Helpline has handled related to women's rights organizations, 63% were reactionary, with the largest number of cases (23.6%) related to account compromise, followed by harassment (9.4%) and censorship (7.6%).[13] The platforms where women faced the most attacks were Facebook (20.5% of cases), followed by Twitter (10.3%), then Instagram (8.9%).

8. In particular, highly visible women, and those in leadership positions, face targeted harassment. Women politicians are more likely than men to be targeted with "higher volumes of online abuse and disinformation"; moreover, when they are targeted, attacks are "more likely to be steeped in sexism" and "'stickier,' or harder to recover from and fight with traditional tools like fact-checking and media literacy."[14]

---

[10] International Media Support (IMS), Online gendered disinformation and sexist hate speech, 6 March 2023, 4, https://www.mediasupport.org/wp-content/uploads/2023/03/IMS-Online-gendered-disinformation_final.pdf.
[11] United Nations, Declaration on the Elimination of Violence Against Women, General Assembly Resolution 48/104, 20 December 1993, available at: https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.21_declaration%20elimination%20vaw.pdf .
[12] IMS, Online gendered disinformation and sexist hate speech, 5.
[13] Access Now, Strengthening Civil Society's Defenses: What Access Now's Digital Security Helpline has Learned from ITs first 10,000 Cases, 7 June 2021, 21, available at: https://www.accessnow.org/wp-content/uploads/2021/06/Helpline-10000-cases-report.pdf.
[14] *Ibid.*

9. Gendered disinformation attacks exploit sexist narratives to frame women as unfit for leadership. Common themes of misogynist attacks paint women as untrustworthy, unqualified, unintelligent, and unlikable.[15] Attacks are coordinated with other misinformation tactics, such as "fake polls, forged electoral posters asserting nonexistent political alliances, and unfounded rumors" with the intent of manipulating voters and developing "falsely informed understandings of womens' track records."[16] Gendered disinformation does not spread mere falsities, but also uses "highly emotive and value-laden content to try to undermine its targets."[17]

    a. A study of gendered disinformation in the **Philippines** and **Poland** found that gendered disinformation attacks followed several consistent themes which played on existing tropes, such as convincing the public that women are devious and unfit for politics and unintelligent. For instance, in the Philippines "women journalists – particularly those who are critical of the Duterte government – are the primary targets of disinformation campaigns, dubbed 'presstitutes' for their so-called duplicitous and compromised reporting against Duterte."[18]

    b. In **Ukraine**, Svitlana Zalishchuk had a "harrowing experience with online harassment and fake news."[19] She testified:

> *I myself have experienced the situation when one absurd fake produced by the number of Russian websites was actively picked up in social media and shared by Ukrainian users. Aimed at discrediting me as the politician, the story was suggesting that I made a promise in my FB-post to run naked through Kyiv once the town in the east of Ukraine Debaltseve is taken by the Russian-backed separatists. "Substantiated" with the fake screenshot of the post, the story kept circulating on the Internet for a year, objectifying my sex and distancing discourse about my personality from the professional area.*[20]

    c. In **Latin America**, women's rights groups face attacks online from governments and institutions as well as non-state actors. For instance, a Costa Rican women's rights group was targeted in a phishing attack which they reported to Access Now's Helpline. In the attack, the perpetrator impersonated Facebook staff and claimed that the women's rights group had been reported for violating the site's terms. The attacker sent the group a phishing link and instructed them to follow it to resolve the fake report, in an attempt to compromise the group's Facebook login credentials. Access

[15] #She Persisted, Monetizing Misogyny, 7.
[16] #ShePersisted, From Catalyst for Freedom to Tool for Repression, 10, 14.
[17] Demos, Engendering Hate, 6.
[18] *Ibid.* at 29.
[19] *Ibid.* at 27.
[20] #She Persisted, Women, Politics & Power, 33.

Now acted to warn other CSOs to prevent them from getting attacked and to get the illegitimate Facebook page and phishing site removed.[21]

10. **Gendered disinformation is closely related to gendered malinformation.** In **Tunisia**, gendered malinformation is a strategy of disinformation campaigns to silence women. Highly visible women often fall victim to doxxing "as a part of defamatory campaigns full of hate speech, bullying and inciting violence." Doxxing is a form of malinformation and occurs when personal information is publicly shared without a person's consent. In cases of gendered disinformation, a woman's personal information is weaponized against her to spread disinformation and intimidate her into silence. Throughout the MENA region, "[doxxing is] a repressive and violent tactic against women used by many governments and their security apparatus…they are telling women: dare to speak up, and you will be scandalized."[22]

11. **Social media companies' problematic business models** is a fundamental factor behind disinformation, including gendered disinformation.[23] Importantly, these companies profit from harmful narratives of women that are "boosted and amplified through algorithms that make such content sticky and often viral, through recommender systems that are built to maximize attention and features that facilitate its rapid and widespread distribution."[24] The main methods of manipulation that platforms engage in that harm fundamental rights are surveillance-based advertisement, including political advertising, and amplification of disinformation online via content recommender systems and personalisation of news content.[25]

    a. In **Brazil**, Coding Rights – a nonprofit advancing an intersectional, feminist approach to defending human rights in the development, regulation, and use of technologies – highlights how social media companies have profited from disinformation. "Hate speech, gender-based political violence and misinformation about electoral procedures are all promoted and monetised by their algorithms that prioritise engagement, while being biased against LGBTIQA+ and other vulnerabilised communities."[26]

    b. In a study of gendered misinformation campaigns against women in politics in **Brazil**, **Hungary**, **Italy**, **India**, and **Tunisia**, the design of social media platforms was found "largely responsible for the current hellscape experienced by women online."[27]

[21] Access Now, Strengthening Civil Society's Defenses, 23.
[22] #ShePersisted, From Catalyst for Freedom to Tool for Repression, 12.
[23] Access Now, Informing the Disinfo Debate: A Policy Guide for Protecting Human Rights, December 2021, 4, available at: https://www.accessnow.org/wp-content/uploads/2021/12/Informing-the-disinfo-debate-report.pdf .
[24] #ShePersisted, Monetizing Misogyny, 5.
[25] Access Now, Informing the Disinformation Debate, 5.
[26] Coding Rights, Coding Rights and APC Internvention at the GDC Americas Multistakeholder Consultation, 15 Feburary 2023, available at: https://codingrights.org/en/library-item/coding-rights-and-apc-intervention-at-the-gdc-americas-multistakeholder-consultation/.
[27] #ShePersisted, Monetizing Misogyny, 5.

Moreover, these companies repeatedly refused to act in combating gendered misinformation."[28]

B. Gendered surveillance as a tactic of gender disinformation

12. Worldwide, WHRDs are targeted through digital surveillance. Gendered surveillance is closely related to gender disinformation campaigns and is used as a tactic to silence women and gender justice advocates. Digital surveillance against women takes the form of both state and social surveillance.[29] State surveillance is backed by state machinery such as government institutions or intelligence agencies. Increasingly, state surveillance is conducted through the use of targeted tools and services procured from commercial entities, like the NSO Group and its infamous Pegasus software. Social surveillance, on the other hand, is "monitoring and contact by social actors who have the effect of surveilling, policing, threatening and influencing the work of journalists" and other WHRDs.[30] Rather than being discrete categories, "the two work together in complicated ways to harass, threaten and monitor journalists."[31] As one example, targeted surveillance may be used to exfiltrate information from the targeted person's device or accounts, in order to later be deployed in concerted malinformation campaigns against them publicly.

13. Last year, Access Now and Front Line Defenders[32] published a report, *Unsafe anywhere: women human rights defenders speak about Pegasus attacks*, detailing the first-hand experiences of women victims/survivors of state-sponsored spyware attacks. The report exposed the gendered aspects of surveillance, as well as sharing testimonials of women targeted by Pegasus.[33]

14. Through the main stories of two women journalists targeted in Jordan and Bahrain, the report illustrated how "the impact of targeted surveillance on women can be particularly grievous, given that political, societal, and gender power asymmetries often grant authorities opportunities to weaponize the information they extract through defamation, blackmail, and doxxing."[34]

    a. In **Bahrain**, One victim of Pegasus surveillance, Ebtisam Al-Saegh, expressed that "personal freedoms are over for me, they no longer exist. I am not safe at home, on the

[28] *Ibid.* at 4.
[29] Digital Rights Foundation, Surveillance of Female Journalists in Pakistan: a Research Study by Digital Rights Foundation, May 2023, https://digitalrightsfoundation.pk/wp-content/uploads/2017/02/Surveillance-of-Female-Journalists-in-Pakistan-1.pdf.
[30] *Ibid.*
[31] *Ibid.* at 8.
[32] Front Line Defenders is an international human rights NGO that improves the security and protection of human rights defenders "at risk for their peaceful and legitimate human rights work." *See* Front Line Defenders, About Us, available at: https://www.frontlinedefenders.org/en/who-we-are .
[33] Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks.
[34] *Ibid.*

street, or anywhere."[35] A renowned WHRD who works for SALAM Democracy and Human Rights in Bahrain, Al-Saegh was targeted when her "iPhone was hacked at least eight times between August and November 2019 with NSO Group's Pegasus spyware." **Jordanian** human rights lawyer Hala Ahed Beeb "who has worked with a number of human rights and feminist organizations to defend women's and workers' rights, and freedom of expression in her country" was also targeted with Pegasus. Both women "live in fear of how their personal information, such as private photos, videos, and conversations, could be used to harass and abuse them."[36] In the Middle East and North Africa (MENA) region, many WHRDs continue to be victims of spyware attacks, including "Emirati activist Alaa Al-Siddiq, Al Araby journalist Rania Dridi, and Al Jazeera broadcast journalist Ghada Oueiss."[37] A UN study of Women in Arab States found that "70% percent of women activists and WHRDs in the region reported feeling 'unsafe online' after receiving insulting and hateful messages and unwanted sexual content and communications, and 35% of them reported the existence of a continuum 'between online and offline VAWG,' highlighting the very real dangers that can stem from violent speech on social media."[38]

b. In **India**, the Internet Democracy Project (IDP) called Pegasus spyware and surveillance of journalists "deeply concerning for women who speak up against powerful men."[39] In 2021, a group of 500 activists and academics submitted a letter appealing to the Chief Justice of India demanding an independent and transparent investigation into India's alleged purchase and use of Pegasus. In particular, the letter focused on "the alleged snooping on a Supreme Court staffer who accused ex-CJI Ranjan Gogoi of sexual harassment in 2019." As Radhika Radhakrishnan of IDP observed, surveillance has high stakes for women: "misuse of this data would not just be a data violation, but could easily extend to voyeurism, slut-shaming, and predatory actions, which threaten a woman's bodily integrity."[40]

c. In **Pakistan**, the Digital Rights Foundation (DRF) found that "in line with past years' trends, women were the highest reported victims of online harassment at 58.6%" in 2022.[41] Among cases of cyber harassment of women, journalists were the most targeted profession, then activists, and then lawyers. Women journalists face gendered

[35] *Ibid.*
[36] Access Now, Unsafe anywhere: attacked by Pegasus, women activists speak out, 17 January 2022, available at: https://www.accessnow.org/press-release/pegasus-women-activists/.
[37] Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks.
[38] #ShePersisted, From Catalyst for Freedom to Tool for Repression: a #ShePersisted Analysis of Gendered Disinformation in Tunisia, July 2023, 12.
[39] Internet Democracy Project, Pegasus Surveillance is Deeply Concerning for Women Who Speak Up Against Powerful Men, 2021, available at: https://internetdemocracy.in/media/pegasus-surveillance-is-deeply-concerning-for-women-who-speak-up-against-powerful-men-activists-say.
[40] *Ibid.*
[41] Digital Rights Foundation, Cyber Harassment Helpline: Annual Report 2022, February 2023, 13, available at: https://digitalrightsfoundation.pk/wp-content/uploads/2023/05/Cyber-Harassment-Helpline-Annual-Report-2022-1.pdf.

forms of state and social surveillance. In cases of state-backed surveillance, malign actors employed "sexualized threats or the possibility of revealing facts about their personal lives" to intimidate and harass journalists.[42] Social surveillance against women journalists is also pervasive.[43] Many journalists interviewed by DRF agreed that "talking about violence against women and problems that women face in society results in a lot of online abuse."[44]

d. In the **Dominican Republic**, Pegasus software was discovered on the cell phone of a prominent woman journalist, Nuria Piera, who "was working on sensitive, high-profile investigations around the time her device was infected."[45] Following the attack, Piera discussed its impact:

> *You have to work hard to not become neurotic, because you're always suspicious that someone may have information about you. It's like being in quicksand. It really affects your sense of freedom, how free you feel to speak up. Sometimes you don't even know how they want to hurt you, through you or through your loved ones. You then feel responsible, which is even more serious.*[46]

e. In the **United States**, many women in politics are victims of social surveillance in the form of "armies of often politically motivated trolls and bots."[47] The former Women's Vote Director for Hillary Clinton's 2016 presidential campaign Mini Timmaraju reported:

> *I would often post about women's events, policy positions of interest to our women supporters and updates from our women surrogates. I noticed that as I became more active and gained more followers, I was increasingly followed by trolls and obvious bots, posting inflammatory replies and comments to intimidate and harass our female followers. It made me realize that the amount of energy that a woman has to spend online to defend her positions and her reputation is just overwhelming.*[48]

15. These attacks are not isolated incidents. In January 2022, Citizen Lab and Access Now published a joint report "confirming the use of Pegasus against journalists and members of

[42] Digital Rights Foundation, Surveillance of Female Journalists in Pakistan, 19.
[43] *Ibid.*
[44] *Ibid.* at 17.
[45] Amnesty International, Dominican Republic: Pegasus spyware discovered on prominent journalist's phone, 2 May 2023, available at: https://www.amnesty.org/en/latest/news/2023/05/dominican-republic-pegasus-spyware-journalists-phone/.
[46] *Ibid.*
[47] #ShePersisted, Women, Politics & Power in the New Media World, Fall 2019, 32, available at: https://www.iknowpolitics.org/sites/default/files/191105shepersisted_final.pdf.
[48] *Ibid.*

CSOs in El Salvador on a massive scale."[49] Prior to this report, The Pegasus Project uncovered the systemic misuse of Pegasus threatened people in over 50 countries.[50]

16. These findings all underscore that surveillance is inherently gendered, and is a tactic of gendered disinformation. Targeted surveillance of WHRDs is part of a broader aim to minimize, stigmatize, and deter women from participating in public spaces.[51] Surveillance often has the goal of control.[52] New technologies have allowed state and non-state actors to deepen scrutiny of women in the digital age.[53] As Internet Democracy Project states,

> *By gendering surveillance, perpetrators can really bring home the harms of surveillance. Indeed, surveillance of women is a long-standing practice in our society as elsewhere - and one that women from all castes, classes and religions are too familiar with, even if it affects them differently.*[54]

II. Effects of 'gendered disinformation' on individual well-being and democracy

17. The impacts of gendered disinformation on an individual and societal level are wide ranging and severe. On an individual scale, women targets of gendered disinformation attacks report heavy mental health tolls, and a chilling effect on "their activism and their willingness and ability to express themselves online."[55] In terms of democracy, gendered disinformation chills womens' exercise of their freedom of expression. As a consequence of public participation, "women face the weaponization of information that directly impacts their opportunities for leadership and participation."[56] Deterring women from public participation greatly undermines democracy.

A. Impacts on individual well being

18. On an individual scale, victims of gendered surveillance report declining mental health, social isolation, and restrictions on freedom of movement due to fear of physical harassment and threat. Spyware attacks have devastating impacts on their victims, and they are particularly severe for women. Pegasus spyware "not only strips women of privacy, the surveillance also

[49] Amnesty International, Dominican Republic: Pegasus spyware discovered; See Access Now and Citizen Lab, Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware, 12 January 2022, available at: https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware .
[50] Forbidden Stories, About the Pegasus Project, available at: https://forbiddenstories.org/about-the-pegasus-project/.
[51] Internet Democracy Project, Gendering Surveillance: An Introduction, February 2017, available at: https://genderingsurveillance.internetdemocracy.in/intro/.
[52] Access Now, The gender of surveillance: how the world can work together for a safer internet, 6 February 2018, available at: https://www.accessnow.org/gender-surveillance-world-can-work-together-safer-internet/.
[53] Access Now, Internet Democracy Project: Fighting gendered surveillance and access disparities in India, 28 March 2018, available at: https://www.accessnow.org/internet-democracy-project/ .
[54] Internet democracy Project, Gendering Surveillance.
[55] *Ibid.* at 8.
[56] Demos, Engendering Hate.

destroys the inviolability of their homes and immediate surroundings."[57] A target's friends, relatives, and social network is also likely impacted as people close to a victim may fear being harmed or surveilled.

19. Women victims of spyware attacks report restrictions on freedom of movement out of fear of physical threat or harassment. From 2015-2020, Emirati activist Alla Al-Siddiq's phone was hacked multiple times using Pegasus software. "Before Alaa Al-Siddiq's tragic death…one of her friends testified to how she changed her habits in fear of surveillance, including "changing routes she traveled on the tube. She tried to be mindful to not stand too close to the edge when she was traveling by train, for fear she could be pushed [onto] the tracks."[58]

20. Targeted harassment also carries specific and grave individual harms. Online GBV and disinformation is part of a "continuum of violence that women and girls experience throughout their life course and cannot be separate from 'offline' violence."[59] As the murder of Jo Cox in the United Kingdom demonstrated, "at times, online threats turn into physical violence and even political murder, as sexist attitudes and beliefs have been found to be the factors most strongly associated with the support for violent extremism."

B. Impacts on Democracy

21. By employing gendered surveillance, targeted harassment, and other tactics, gendered disinformation campaigns erode a range of human rights and threaten womens' freedom of expression and civic engagement. "To evade the very public and dangerous attacks facilitated by social media, women may also disengage from politics or self-censor and refrain from speaking out on women's rights and individual liberties."[60] In the long run, this harms the advancement of gender justice and women's rights issues since "there is significant overlap between disinformation campaigns, misogynistic discourse, backlash, roll back on gender equality and women's rights and the erosion of democratic principles, including the reshaping of democracy through social media."[61]

22. In its submission to the UN Special Rapporteur on the freedom of opinion and expression on gender justice and FOE, the Association for Progressive Communications elaborated how disinformation harms democracy:

> *Disinformation causes confusion and has a chilling effect on freedom of expression and information. It directly impacts on the level of trust in the public sphere as a space for*

[57] Access Now, Unsafe anywhere: women human rights defenders speak out about Pegasus attacks.
[58] *Ibid.*
[59] Wilton Park, Building a shared agenda on the evidence base for Gender-Based Online Harassment and Abuse, August 2022, 3.
[60] #ShePersisted, From Catalyst for Freedom to Tool for Repression, 14.
[61] Wilton Park, Building a shared agenda, 5.

democratic deliberation. People no longer feel safe to express their ideas for fear of online harassment and of being targeted by disinformation campaigns; others feel paralysed and silenced by the puzzlement and uncertainty created by the surrounding information pollution and remove themselves from public debate concerning key issues of public interest.[62]

23. Gendered disinformation also harms democracy by discouraging women generally from exercising their rights. As expressed by the US State Department, "one goal of [targeting women and people with intersecting identities] is to dissuade individuals from practicing their freedom to express and uphold beliefs and ideals that contradict their adversaries' beliefs."[63] Another consequence of gendered disinformation is "to dissuade members of broader identity-based groups from exercising their rights."[64] Ultimately, gendered disinformation threatens democracy "by undermining the ability to access impartial, fact-based information, and it negatively impacts the make-up of democratic representation."[65]

24. Gendered disinformation has chilling effects on women journalists' freedom of expression and impacts what topics are covered. In its study of women journalists who faced cyber harassment in Pakistan, Digital Rights Foundation found that "surveillance has a direct impact on what journalists say and the subjects that they work on, which has implications for free speech and freedom of the press."[66]

III. Responses

A. Measures States, digital companies and international organizations have taken to combat 'gendered disinformation'

25. **States.** Governments have taken several actions against spyware. In the **United States**, the White House issued an Executive Order in March 2023 titled the Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security. The Order states "as the policy of the United States Government that it shall not make operational use of commercial spyware that poses significant counterintelligence or security risks to the United States Government or significant risks of improper use by a foreign government or

[62] Association for Progressive Communications, Gender Justice and the Right to Freedom of Opinion and Expression, June 2021, available at: https://www.apc.org/sites/default/files/APC_submission_on_gender_justice_and_the_right_to_freedom_of_opinion_and_expression.pdf.
[63] U.S. Department of State, Gendered Disinformation.
[64] *Ibid.*
[65] *Ibid.*
[66] Digital Rights Foundation, Surveillance of Female Journalists in Pakistan, 6.

foreign person."[67] Last year, **Costa Rica** was the first country to call for a moratorium on spyware technology.[68]

26. The Freedom Online Coalition, with **37 member states,** asserts in its guiding principles on government use of surveillance technologies that "governments should not use these surveillance technologies to unjustifiably interfere with freedom of expression; discourage the exercise of human rights and fundamental freedoms; perpetrate technology-facilitated gender-based violence or discrimination online and offline; perpetuate harmful or discriminatory norms and stereotypes; or limit bodily autonomy through any means, including but not limited to unlawful collection or misuse of personal health data, including reproductive and sexual data, or distribution of intimate images."[69]

27. **Digital companies.** Social media platforms' problematic business models are largely responsible for the extent of gendered disinformation campaigns. As organizations like #ShePersisted and Access Now have shown, companies have repeatedly failed to address gendered disinformation despite "providing illiberal actors new, exceptionally powerful tools to attack citizens and undermine human rights and democracy, further marginalizing those voices they find threatening."[70] To date, technology companies have not implemented user safety, accountability and transparency protocols, and the problem is acute especially in Global South nations.[71]

28. **International organizations.** So far, efforts by supranational, international, and multilateral organizations to combat disinformation have missed the mark. The European Union's Code of Practice on Disinformation does not address platforms' problematic business models as a foundational matter in addressing disinformation.[72] In 2022, the Global Partnership for Action on Gender Based Online Harassment and Abuse convened to address online GBV in three ways: developing and advancing shared principles, increasing targeted programming and resources, and expanding reliable, comparable data and access to it.[73]

---

[67] Executive Order on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security, 27 March 2023, available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/#:~:text=Therefore%2C%20I%20hereby%20establish%20as,foreign%20government%20or%20foreign%20person.

[68] Access Now, Stop Pegasus: Costa Rica is the first country to call for a moratorium on spyware technology, 13 April 2022, available at: https://www.accessnow.org/press-release/costa-rica-first-country-moratorium-spyware/.

[69] Freedom Online Coalition, Guiding Principles on Government Use of Surveillance Technologies, March 2023, 2, available at: https://freedomonlinecoalition.com/wp-content/uploads/2023/03/FOC_Guiding_Principles_on_Government_Use_of_Surveillance_Technologies.pdf

[70] #ShePersisted, Monetizing Misogyny, 4.

[71] #ShePersisted, From Catalyst for Freedom to Tool for Repression, 21.

[72] Access Now, Informing the Disinformation Debate, 4.

[73] U.S. Department of State, 2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse, 16 March 2022, available at: https://www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/.

29. **CSOs.** Several CSO initiatives have filled gaps that these other stakeholders have not addressed. #ShePersisted offers support for women politicians facing gendered disinformation. Several other organizations, such as Access Now's Helpline, Internet Democracy Project (which researches gendered surveillance), Digital Rights Foundation's cyber harassment helpline, and several Latin American organizations[74] combat cyber harassment of women. This is not an exhaustive list. However, pervasive narratives that hide the problem of GBV and gendered disinformation still stand in the way of systemic solutions.[75]

Recommendations

Gendered disinformation is a complicated, multi-faceted issue. Any response to tackling the problem cannot be monolithic and must center and learn from the experiences of women who are already working to challenge disinformation. We therefore recommend that the UN Special Rapporteur consider the following recommendations:

1. **States**
    a. Implement an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards that center on gender are put in place. Where there is evidence that commercial spyware technology facilitates or enables human rights abuses, implement a ban on the technology and its vendors;
    b. strengthen control of public funds that are currently misused to fuel state propaganda online while also developing or expanding funding beyond Big Tech to fund independent research and programming, carried out by organizations which are financially independent from Big Tech, and therefore have the ability to speak truth to power;
    c. Phase out behavioral advertising and profiling, and provide greater control and transparency to people on content moderation and algorithmic decision-making. Integrate fully gendered perspectives into policies and programs to address gendered disinformation.

2. **Private sector** (applicable to both the private sector and the investors of the private sector)
    a. Implement effective measures for transparency and accountability towards individuals, and provide access to effective remedies;
    b. Engage local expertise when moderating content, detecting gendered disinformation and developing counter-disinformation, protection, and resilience efforts;
    c. Incentivize platforms to rigorously implement their own terms of service when it comes to threats, harassment, doxing, and manipulated imagery;

[74] Access Now, Six Latin American activist organizations you can support for International Women's Day, 8 March 2021, available at: https://www.accessnow.org/international-womens-day/
[75] Access Now, The gender of surveillance: how the world can work together for a safer internet.

d. Phase out advertising that is based on tracking and targeting via profiles assembled with personal data, including inferred data, to minimize facilitation of gendered disinformation;
e. In the transition to phasing out surveillance-based advertising, limit targeting methods to the minimum and provide transparency on the current targeting methods;
f. Mandate accountability for platforms' delivery algorithms to help ensure proper oversight;
g. Support digital and media literacy, closing the digital gender divide, to minimize the impact of gendered disinformation.

3. International organizations

a. Highlight gendered surveillance, targeted harassment, and other tactics of gendered disinformation through interventions and resolutions at the Human Rights Council, General Assembly, and other UN fora;
b. Engage with the Office of the High Commissioner for Human Rights and Special Procedures to monitor, maintain pressure, and ensure UN action on the matter;
c. Take concrete steps to ensure independent and accessible legal avenues for complaints, both domestically and internationally, are available for victims of gendered disinformation;
d. Join civil society's efforts in support for regulating surveillance technologies and social media platforms.

Access Now (https://www.accessnow.org) defends and extends the digital rights of individuals and communities around the world. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

*For more information, please contact: **un@accessnow.org***