Ponder the Improbable since 1996

GENDER, SECURITY AND DIGITAL SPACE

ISSUES, POLICIES, AND THE WAY FORWARD

Policy Report

December 2021

Gulizar Haciyakupoglu
and Yasmine Wong

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Policy Report

GENDER, SECURITY AND DIGITAL SPACE

ISSUES, POLICIES, AND THE WAY FORWARD

Gulizar Haciyakupoglu and Yasmine Wong

December 2021

TABLE OF CONTENTS

Executive Summary

Online threats are often approached without a gender focus, despite having disproportionate impacts across different genders. Gender-based online threats, including gendered disinformation (disinformation with gender-specific undertones) and harassment, can build on gender stereotypes and deepen existing faultlines in societies. Foreign influence attempts or domestic power politics may exploit these gender-related faultlines, and they can hamper democratic participation by women and marginalised groups. Furthermore, the digital divide and internet shutdowns, both of which have gendered impacts, may restrict certain gender groups from accessing economic opportunities, legal aid and information, and self-help, among others. The gendered implications of these threats impair the myriad of opportunities that Information and Communication Technologies could otherwise provide to advance gender equality. Building on the 2021 CENS & The High Commission of Canada Webinar Series on “Gender, Security and Digital Space”, this policy report reiterates the need to embrace a gender-focused approach to studying cybersecurity threats to understand and tackle their gender-specific impacts. The policy report ends with a discussion on the actions that can be taken by the government, social media companies, and society to alleviate the problem.

Gender, Security and Digital Space: Issues, Policies, and the Way Forward

Information and Communication Technologies (ICTs), under the right circumstances, provide opportunities to advance gender equality.[1] This includes amenities for political engagement, freedom of expression, and income equality.[2] It also offers spaces for women to articulate their concerns, for marginalised politicians to connect with their voter base,[3] and for individuals to access self-help and support groups. However, online threats including harassment, disinformation, and internet shutdowns undermine the equalising potential of ICTs because of their gendered impacts.[4]

It is timely to explore online threats through gendered lens. Efforts to build societal awareness of the dangers of online abuse,[5] disinformation, and hate speech is growing. At the same time, experts are working hard to draw attention to gendered disinformation (disinformation with gender-specific undertones) and harassment, as well as other issues and threats at the intersection of gender, security, and digital space.

This policy report first provides an overview of how online threats can have gendered implications and why it is necessary to embrace a gender-focused perspective when evaluating individual and national security concerns online. Subsequently, it shares policy considerations. The report builds on the presentations delivered in the three-part webinar series on "Gender,

[1] As recognised by many speakers at the "Gender, Security and Digital Space" Webinar Series, "CENS & The High Commission of Canada Webinar Series on 'Gender, Security and Digital Space: Exploring Risks, Opportunities, and Security Implications' (May 11, 18 & 25),"10 August 2021, https://www.rsis.edu.sg/rsis-publication/cens/cens-the-high-commission-of-canada-webinar-series-on-gender-security-and-digital-space-exploring-risks-opportunities-and-security-implications/?doing_wp_cron=1628575302.1500000953674316406250#.YRIgUIgzaM; Mitali Mukherjee, Aditi Ratho and Shruti Jain, "Unsocial Media: Inclusion, Representation, and Safety for Women on Social Networking Platforms," ORF Occasional Paper No. 312, May 2021, Observer Research Foundation. https://www.orfonline.org/research/unsocial-media/.

[2] Sarah Shoker, "Gender, Internet Shutdowns, & International Security," Panel 1, 11 May 2021, in "CENS & The High Commission of Canada Webinar Series" pg. 16-19; Mitali Mukherjee, Aditi Ratho and Shruti Jain, May 2021.

[3] Lucina Di Meco, "#ShePersisted Women, Politics and Power in the New Media World," 2019, p. 23, 24, https://static1.squarespace.com/static/5dba105f102367021c44b63f/t/5dc431aac6bd4e7913c45f7d/1573138953986/191106+SHEPERSISTED_Final.pdf.

[4] i.e., variance in impacts based on gender; "CENS & The High Commission of Canada Webinar Series"; Di Meco, 2019.

[5] The definitions of online abuse, online harassment and hate speech vary across sources. Online abuse and harassment are often used interchangeably and, in some resources, hate speech appears as a component of online abuse.

Security and Digital Space" co-organised by the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU) and the Canadian High Commission.[6] This serves as a prelude to an upcoming edited volume (Gulizar Haciyakupoglu, Yasmine Wong, and Benjamin Ang eds.) which will expand upon and address the issues introduced in this report.

Security Concerns in Cyberspace through Gendered Lens

Feminist perspectives on international relations and security have long introduced the gender question in an arena traditionally dominated by masculine norms, where realist orthodoxy remains influential to the discipline.[7] Feminist approaches to human security, for example, focus on the multiplicity of identities and experiences beyond that of the male subject.[8] Feminist theories have also served to interrogate the gender power relations surrounding technologies.[9]

In the same vein, gender-focused approaches to online security threats aim to locate processes biased towards or shaped in accordance with the thinking of a particular gender when evaluating national and individual security concerns online. This is to remedy inequalities and threats that may arise from the use, design, and governance of digital technologies premised on patriarchal norms.

The assumption that cyberspace is gender neutral overlooks "differences in the capabilities, needs, and priorities" across genders and how gender norms undergird priorities within cybersecurity designs,[10] where systems are often designed with the average male user in mind.[11] For instance, various cybersecurity measures to safeguard individuals against privacy violation and identity theft base password backup on personal information (e.g., mother's

[6] "CENS & The High Commission of Canada Webinar Series."

[7] Anuradha M. Chenoy, "Bringing Gender into National Security and International Relations", *INTERNATIONAL STUDIES*, 37(1) (2000). 17-29.

[8] Heidi Hudson, "'Doing' Security As Though Humans Matter: A Feminist Perspective on Gender and the Politics of Human Security", *Security Dialogue*, 36(2) (2005), 155-174; Natasha Marhia, "Some humans are more *Human* than Others: Troubling the 'human' in human security from a critical feminist perspective", *Security Dialogue*, 44(1) (2013), 19-35; Maria Stern and Annick Wibben, "A decade of feminist security studies revisited", *Security Dialogue*, Special Virtual Issue, 1-6.

[9] Judy Wajcman, "Feminist theories of technology", *Cambridge Journal of Economics*, Vol. 34(1) (2010), 143-152.

[10] Katharine M. Millar, "Gendered Approaches to Cyber Security," Panel 1, 11 May 2021, in "CENS & The High Commission of Canada Webinar Series", p. 9-12.

[11] Ibid.

maiden name or name of first pet), neglecting the risk from an intimate partner or close contact who has access to the victim's personal information.[12] This especially affects women who are suffering intimate partner or family violence and imposes additional security burdens on them.[13] In addition to such design related issues, gender-based implications of online threats like harassment, disinformation, and impediments to internet access bring about individual and national security risks as discussed below.

A recent Pew Research Center survey on online harassment faced by adults in the US revealed that four out of ten respondents have been victims, with gender influencing the types of harassment experienced.[14] Harassment against men involved offensive name-calling and physical threats more often than women, while women were more likely than men to "report having been sexually harassed online or stalked."[15] Lesbian, gay, and bisexual individuals were particularly vulnerable, with seven in ten having experienced online harassment.[16]

Disinformation can also have gendered impacts. Gendered disinformation includes false information or misleading visuals that often build on existing gender stereotypes and that can be used to deter women and marginalised groups from participating in politics and the public sphere,[17] which in turn harms democracy.[18] Multiple studies highlighted how female politicians, journalists, and public figures are targeted with gendered disinformation.[19] Some

[12] Katharine MIllar, James Shires and Tatiana Tropina, "Gender approaches to cybersecurity: design, defence and response, Geneva, Switzerland: United Nations Institute for Disarmament Research (2021); Katharine Millar, 11 May 2021.

[13] Ibid.

[14] Emily A. Vogels, "The State of Online Harassment," Pew Research Center, 13 January 2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

[15] Ibid.

[16] Ibid.

[17] Nina Jankowicz, "Malign Creativity: How Gender, Sex, and Lies Are Weaponised Against Women Online," Panel 2, 18 May 2021, in "CENS & The High Commission of Canada Webinar Series", p. 28-32; "Defining the Problem," #Shepersisted, https://www.she-persisted.org/why; "CENS & The High Commission of Canada Webinar Series."

[18] Nina Jankowicz, 18 May 2021; Lucina Di Meco, 18 May 2021; Gabrielle Bardall, 18 May 2021.

[19] Nina Jankowicz, Jillian Hunchak, Alexandra Pavliuc, Celia Davies, Shannon Pierson and Zoe Kaufmann, "Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online", The Wilson Centre, Science and Technology Innovation Program, January 2021, https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online; Lucina Di Meco, "Gendered Disinformation, Fake News, and Women in Politics", Council on Foreign Relations, 6 December 2019, https://www.cfr.org/blog/gendered-disinformation-fake-news-and-women-politics; Bonnie Stabile, Aubrey Grant, Hemant Purohit and Kelsey Harris, "Sex, Lies, and Stereotypes: Gendered Implications of Fake News for Women in Politics", Public Integrity, vol. 21 issue 5, 2019, https://doi.org/10.1080/10999922.2019.1626695; Julie Posetti, Nabeelah Shabbir, Diana Maynard, and Kalina Bontcheva, and Nermine Aboulex, "The Chilling: Global trends in online violence against women journalists," UNESCO, April 2021, https://unesdoc.unesco.org/ark:/48223/pf0000377223

also identified intersections among gender, race, and ethnicity-based negative or misleading narratives,[20] such as those targeted at US Vice President Kamala Harris.[21] Furthermore, foreign influence attempts can capitalise on gendered narratives to create fissures within the population and instil fear of social change.[22] For instance, some argue that Russia has employed gender-based narratives in certain foreign influence attempts, including the disinformation campaign targeting Ukrainian politician Svitlana Zalishchuk and Finnish journalist Jessikka Aro.[23]

State attempts to manage and govern the internet is yet another issue that has created vulnerabilities for women. For instance, in India, where the state has used internet shutdowns in the name of "national security and public safety" or in "fighting fake news and hate speech", access to legal help[24] and information was restricted during shutdowns, which had disproportionate effects on women who relied on cyberspace to access public services.[25] In addition, there were concerns that women sharing the house with their abusers could struggle to reach for help when the internet is down, while a domestic abuse victim stated that she struggled to reach her lawyer in the absence of an internet connection.[26]

More fundamentally, some countries struggle with basic access to digital technology, with women and girls facing greater inequality in the digital divide. This divide impinges on women's ability to access new markets,

[20] Cécile Guerin and Eisha Maharasingam-Shah, "Public Figures, Public Rage: Candidate abuse on social media," Institute for Strategic Dialogue, 2020, https://www.isdglobal.org/wp-content/uploads/2020/10/Public-Figures-Public-Rage-4.pdf; Emily A. Vogels, "The State of Online Harassment," Pew Research Center, 13 January 2021, https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/; Nina Jankowicz et. al., January 2021; Priyank Mathur, 25 May 2021; Nina Jankowicz, 18 May 2021.

[21] Jankowics et. al, January 2021; Noah Bierman, "Black, female and high-profile, Kamala Harris is a top target in online fever swamps", *Los Angeles Times*, 19 February 2021, https://www.latimes.com/politics/story/2021-02-19/kamala-harris-is-the-top-target-of-online-harassment-as-fears-of-political-violence-grow.

[22] Samantha Bradshaw (2019) as cited in Bradshaw, "Influence Operations and Disinformation on Social Media", *CIGI Online*, 23 November 2020, https://www.cigionline.org/articles/influence-operations-and-disinformation-social-media/; Gabrielle Bardall, 18 May 2021, p. 23.

[23] As cited in Nina Jankowicz et. al., January 2021, p. 34.

[24] Neo Chai Chin, "Helplessness, hopelessness: The human cost of India's Internet shutdowns," Channel News Asia, 23 March 2021, https://www.channelnewsasia.com/news/cnainsider/helpless-hopeless-human-cost-india-internet-shutdowns-kashmir-14467916.

[25] "India's internet shutdowns function like 'invisibility cloaks'," DW, 13 November 2020, https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554.

[26] Ibid.

"Bridging the gender divide," ITU, November 2019, https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx; Fitriani B. Timur, "ASEAN Gender Digital Disparities," Panel 1, 11 May 2021, in education, and career opportunities, as well as health and financial services.[27] Unfortunately, in contexts where access is a challenge, gendered implications of online security concerns may remain on the periphery of political agendas.

Current conversations about gender and cybersecurity have mostly been focused on increasing women's participation in science, technology, engineering, and mathematics (STEM) and cybersecurity workforce. However, as the examples above demonstrate, the gender impacts of online threats and inequalities transcend gender parity in STEM and cybersecurity employment, and a gender-focused approach has to be expanded to address the issue of online harms and cyberthreats as a whole.

Policy Considerations

Societies need a gender-focused approach to the design and operation of technological systems, and when identifying and tackling security concerns plaguing cyberspace. Accomplishing this demands a multipronged approach that involves governments, social media companies, and civil society.

The Role of Governments

States need to protect their critical infrastructure, and social and political well-being concurrently. While doing so they need to take gendered impacts of online threats into account, as neglecting them would result in cybersecurity designs with limitations, thus endangering a segment of the society and running the risk of eroding the social fabric over time. Experts working on gender-based safety in cyberspace have invited governments to invest in digital inclusion,[28] consider social media laws,[29] and tackle the barriers to addressing gender-based threats.[30]

[27] "Bridging the gender divide," ITU, November 2019, https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx; Fitriani B. Timur, "ASEAN Gender Digital Disparities," Panel 1, 11 May 2021, in "CENS & The High Commission of Canada Webinar Series."

[28] Audrey Tang, "Humor over Rumour," Panel 3, 25 May 2021, in "CENS & The High Commission of Canada Webinar Series", p. 32-34; Gallit Dobner, 11 May 2021; Sun Sun Lim, opening remarks, Panel 2, 18 May 2021, in "CENS & The High Commission of Canada Webinar Series", p. 20-21, 10.

[29] Lucina di Meco, 18 May 2021; Gabrielle Bardall, 18 May 2021.

[30] Audrey Tang, 25 May 2021; Gallit Dobner, 11 May 2021.

On digital inclusion, governments can invest in programmes, and partner with civil society and social media companies to equip women and marginalised individuals with access to digital technologies and skills, including information literacy, to navigate such spaces.[31] For instance, in Singapore, some grassroots initiatives collected and refurbished laptops and distributed them to families who needed the gadgets for work or educational purposes during the pandemic.[32] They also installed security software on the laptops and taught cyber wellness and internet safety to beneficiaries.[33] Governments can help turn such initiatives to sustainable programmes.

Governments and societies must have the means to hold social media companies accountable where necessary, especially when claims of social media companies undervaluing gendered threats are mounting. Recently, whistleblower Frances Haugen shared internal Facebook research exposing Instagram's negative impacts on the mental health of younger users, teenage girls in particular.[34] Testifying before the US Congress, Haugen argued that the company prioritises profit over people's safety.[35] Mark Zuckerberg countered the allegations over a Facebook post,[36] while Nick Clegg, Vice President of Global Affairs at Facebook, announced that the company will introduce features that would encourage teenagers to "take a break" from Instagram and "nudge" teenagers dwelling on content that might "not be conducive to their wellbeing" towards other content.[37]

Amidst rising discontent, some experts see the introduction of laws on social media by governments as part of the solution.[38] Currently, in cases where there are laws on relevant issues such as illegal content, laws and regulation may fail to recognise gendered disinformation and abuse.[39] Besides,

[31] Sun Sun Lim, 18 May 2021; Priyank Mathur, 25 May 2021, Fitriani B. Timur, 11 May 2021; Audrey Tang, 25 May 2021.

[32] Goh Chiew Tong, "Volunteers rush to deliver laptops to families in need before full home-based learning kicks in", *Channel News Asia*, 8 April 2020, https://www.channelnewsasia.com/singapore/covid19-home-based-learning-laptops-volunteers-donation-762616

[33] Ibid.

[34] *Georgia Wells, Jeff Horwitz and Deepa Seetharaman*, "Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show", The Wall Street Journal, 14 September 2021,https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739.

[35] Martin Pengelly and Charles Kaiser, "Facebook whistleblower testimony should prompt new oversight – Schiff", The Guardian, 9 October 2021, https://www.theguardian.com/technology/2021/oct/09/facebook-whistleblower-testimony-frances-haugen-adam-schiff.

[36] Mark Zuckerberg, Facebook, 5 October 2021, https://www.facebook.com/zuck/posts/10113961365418581

[37] "Facebook will try to 'nudge' teens away from harmful content", Reuters, 11 October 2021, https://www.reuters.com/technology/facebook-will-try-nudge-teens-away-harmful-content-2021-10-10/.

[38] Di Meco, 18 May 2021.

[39] Di Meco, 18 May 2021.

without mechanisms to enforce these laws, the efficacy of these laws may be reduced. Relevant government agencies, experts, and civil society can keep an account of the cases where relevant laws are leveraged, how these laws are interpreted in different cases, and which cases did not receive legal attention and why. While a cumbersome task, this would help understand how and when existing laws are implemented and spot the gaps. When drafting and reviewing laws, governments would also need to take into account gendered impacts of online threats – such as how revenge porn impacts women and men differently and calibrate protections accordingly. While doing so, they will need to undertake the arduous task of balancing protecting freedom of speech and regulating against online harms in platforms.

Some governments may lack the political will to tackle the problem.[40] Besides, some governments themselves employ gendered disinformation and abuse against their own population.[41] While domestic and international pressure may nudge some governments to review their behaviours and consider solutions to gender-based online threats, others may ignore them. Some governments may use the notion of "values" to sideline international pressure on issues concerning women and LGBTQ+ rights.[42] In such cases, civil society and other stakeholders have to explore how they can lobby their governments into embracing pressure points, through which governments can be nudged to embrace gender-focused approaches and refrain from pursuing gendered disinformation and abuse.[43]

The Role of Social Media Platforms

Social media companies need to embrace a gender-focused approach. Questions concerning terminology, transparency, and the capacities of machine learning based solutions in responding to gendered threats have been prominent debates in this arena.

[40] Nina Jankowicz, 18 May 2021

[41] Maria Ressa, 25 May 2021; on the use of gendered disinformation as means of state power see Gabrielle Bardall, 18 May 2021.

[42] E.g., Developments in Hungary and Slovenia. Daniel Boffey, "Imposing 'imaginary' values risks EU collapse, Slovenian PM claims," The Guardian, 4 July 2021, https://www.theguardian.com/world/2021/jul/04/imposing-imaginary-values-risks-eu-collapse-slovenian-president-claims; Jennifer Rankin, "Hungary passes law banning LGBT content in schools or kids' TV," The Guardian, 15 June 2021, https://www.theguardian.com/world/2021/jun/15/hungary-passes-law-banning-lbgt-content-in-schools

[43] Maria Ressa, 25 May 2021; Gabrielle Bardall, 18 May 2021.

Various experts have called on social media companies to revisit their definitions of "targeted harassment" as they fall short in addressing comprehensive threats faced by women,[44] and in differentiating various forms of online harassment when drafting solutions to account for their varied targets and impacts.[45] Similarly, some experts highlighted the need to regularly update "classifiers" to identify gendered narratives that escape detection better.[46] There are also calls for social media companies to review and update algorithms with attention to gender to better detect misogyny and hate speech.[47] A central question here concerns what can and cannot be identified with ease using current machine learning systems of the platforms.

Alex Stamos, in a 2019 testimony to the US House of Representatives Committee on Homeland Security, Subcommittee on Intelligence and Counter Terrorism, argued that machine learning performs better in conditions "where there are massive sets of both good and bad content available to train classifier models" (e.g., spam) and on "content for which there are known signatures and general consensus, such as child sexual abuse material".[48] But, it is not perfect against satire or in cases where context is influential.[49] Similarly, Riana Pfefferkorn in a recent study suggested that automated content scanning works better on abuses such as child sex abuse imagery, while user reporting is vital to detecting other types of abuses (including where there is end-to-end encryption).[50]

[44] Nina Jankowicz et. al., January 2021, p. 2, 38; Lucina Di Meco and Saskia Brechenmacher, "Tackling Online Abuse and Disinformation Targeting Women in Politics," Carnegie Endowment, 30 November 2020, https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331; Kirsten Zeiter, Sandra Pepera, and Molly Middlehurst (NDI) and Dr. Derek Ruths (Charitable Analytics International, *Technical lead*), "Analyzing Online Violence Against Women in Politics Report of case study research in Indonesia, Colombia, and Kenya," NDI, 2019, p. 16, 17, https://www.ndi.org/sites/default/files/NDI%20Tweets%20That%20Chill%20Report.pdf.

[45] Gabrielle Bardall, 18 May 2021

[46] Nina Jankowicz et. al., January 2021; Nina Jankowicz, 18 May 2021.

[47] Sun Sun Lim, 18 May 2021.

[48] Alex Stamos, "Prepared Written Testimony and Statement", U.S. House of Representatives Committee on Homeland Security Subcommittee on Intelligence and Counterterrorism on "Artificial Intelligence and Counterterrorism: Possibilities and Limitations", 2019, p. 4, https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/stamos_written_testimony_-_house_homeland_security_committee_-_ai_and_counterterrorism.pdf

[49] Ibid.

[50] Riana Pfefferkorn, "Content-Oblivious Trust and Safety Techniques: Results from a Survey of Online Service Providers", Stanford Internet Observatory, 10 September 2021, https://cyber.fsi.stanford.edu/publication/content-oblivious-trust-and-safety-techniques-results-survey-online-service-providers

[51] Alex Stamos, 2019, p. 3-4.

In his testimony, Stamos provided data from Facebook's community standards enforcement report,[51] where, among others, Facebook spotted 99.3% of terrorist propaganda, 99.2% child nudity and sexual exploitation, and 96.8% of adult nudity and sexual activity related violations "before users reported them".[52] But those concerning hate speech fared at 65.4% while bullying and harassment remained at 14.1%.[53] The data demonstrates the difference between actions that are proactively taken by Facebook, and actions triggered by user reporting on different threats, and to Stamos, this shows the "strengths and weaknesses of Facebook's [and potentially others'] current machine learning systems."[54] In addition, these statistics do not account for the fact that some enforcement actions are more common than others, for example, Facebook takes down approximately 1.76 billion instances of spam compared to four million instances of hate speech.[55]

Both Stamos' and Pfefferkorn's accounts suggest the need for improved reporting mechanisms and elevation of human content management practices to better detect malicious content. Recently, some social media and internet companies (Facebook, Google, Twitter, TikTok) announced various measures to curb violence against women on their platforms, including the enhancement of "reporting" and "curation."[56] Improved reporting features aim to enhance women's experience in "track[ing] and manag[ing] their reports," equip them with "product and policy guidance when reporting abuse," and involve steps concerning context and language.[57] The steps on curation will seek to advance women's "control over who can interact with their posts" and facilitate the use and access to safety features.[58]

The announcement followed a process of consultations with women experts from 35 countries, guided by The Web Foundation.[59] The Web Foundation will observe and report the progress of the companies on this front.[60] These developments are heartening but it will require experts (beyond those already engaged in the process) to observe how and when these promises will be implemented, whether they will create positive impacts, and if there

[52] Ibid, p. 4.

[53] Ibid.

[54] Ibid, p. 3, 4.

[55] Ibid, p. 3.

[56] Katie Collins, "Facebook, Google, TikTok and Twitter commit to tackling abuse of women online," CNET, 1 July 2021, https://www-cnet-com.cdn.ampproject.org/c/s/www.cnet.com/google-amp/news/facebook-google-tiktok-and-twitter-commit-to-tackling-abuse-of-women-online/; Alex Hern, "Social network giants pledge to tackle abuse of women online," The Guardian, 1 July 2021, https://www.theguardian.com/society/2021/jul/01/social-networks-facebook-google-twitter-tiktok-pledge-to-tackle-abuse-of-women-online

[57] Ibid.

[58] Ibid.

[59] Ibid.

[60] Ibid.

will be any geographical prioritisation in implementation. Sadly, accomplishing this and the external vetting of companies' promises may be hampered by transparency-related concerns. As others have also argued, transparency on gender-based harassment, including the number and nature of reported cases and internally identified incidents, and the details of actions taken,[61] would help locate the problems and gaps in response better.

Lastly, companies will likely continue to depend on human content moderation. Social media companies need to constantly invest in hiring, training, and supporting human content moderators to deal with evolving types and modality (text, audio, image, video) of abuse. Furthermore, as discussed above, and as demonstrated by media-facilitated harms against the Rohingya minority in Myanmar, the prevalence of creative ways to escape auto-detection mean that social media companies must hire and equip content moderators with contextual and linguistic knowledge in order to identify malicious content in their areas of focus. In doing so, protecting the mental well-being of content moderators who are exposed to troubling materials is yet another fundamental concern to be addressed.

The Role of (Civil) Society

Civil society organisations (CSO) can fill the societal trust gap and mobilise trusted role models and organisations in response efforts, where trust in government action on the issue is low. Civil society can contribute to the response efforts by raising awareness on the gendered impacts of online threats, taking an active role in the reporting process and by offering support to victims and vulnerable groups.

Efforts to raise awareness should take cultural and contextual specificities into account when tailoring messages and selecting the platform for outreach. CSOs may drive campaigns to make cyber safety tips available to the wider public. While these issues should ideally already feature on governments' priority lists, in some cases, international or domestic pressures might be necessary. Think tanks, scholars, and experts, on the other hand, can help improve the knowledge on and identification of gendered impacts of online threats by introducing the gender aspect into their studies and conferences, and by increasing the number of studies on the topic. This would also partly respond to the need to increase data on "online and ICT-facilitated violence."[62]

[61] Nina Jankowicz, 18 May 2021; Lucina Di Meco and Saskia Brechenmacher, 30 November 2020.

[62] UNWomen, "Online and ICT* facilitated violence against women and girls during COVID-19", 2020, p. 2, https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519

Some experts also call on women to be more vocal about the problem.[63] This would contribute to awareness-raising efforts.

There are also experts who warn that the victims should not bear the burden of reporting harassment alone, especially when perpetrators of gender-based abuse often escape with no consequences and victims are faced with the danger of retaliation.[64] Here, CSOs may step in to amplify the voices of victims and assist in reporting. Some victims may trust CSOs more and prefer consulting with them to avoid retraumatisation from reporting and tracking the outcome of reporting alone. Additionally, if victims report malicious acts to social media companies via CSOs, CSOs may receive information on the types of threats and the intricacies of the reporting process. If CSOs act collectively, they may compile the forms of threats reported to them and gather tangible data points to pressure social media companies and government agencies, to take solid steps based on data, where transparency is currently lacking. Data-backed collective lobbying against threats may have a greater impact than individually-submitted user reports and pressure social media companies and other correspondents to respond timely. There are already some relevant moves[65] and guidelines[66] on this front, but a systematic programme involving CSOs within and across borders could pave the way for more comprehensive and sustainable initiatives.

Safeguards must be put in place before CSOs can assist with reporting and there are limitations to overcome. CSOs would need to establish report-processing standards and agree on guarding ethical considerations, including the protection of the anonymity of those reporting and data security practices. On limitations, some victims may find it easier to report on the platform directly, and CSOs may face a resource (human and financial) crunch to pursue such laborious work. In addition to reporting assistance, civil society and support groups and employers can establish legal, societal, and government-level support and training mechanisms to assist and equip women and marginalised

[63] Lucina Di Meco, 18 May 2021.

[64] Panel 2 (18 May) of the "CENS & The High Commission of Canada Webinar Series."

[65] Jeremy Liebowitz et al. (5 May 2021) speak of reporting and documenting of hate speech by CSO in Burma. Jeremy Liebowitz, Geoffrey Macdonald, Vivek Shivaram, and Sanjendra Vignaraja, "The Digitalization of Hate Speech in South and Southeast Asia: Conflict-Mitigation Approaches", Georgetown Journal of International Affairs, 5 May 2021, https://gjia.georgetown.edu/2021/05/05/the-digitalization-of-hate-speech-in-south-and-southeast-asia-conflict-mitigation-approaches/. European Commission talks about initiatives incorporating CSOs in countering hate speech. "Countering online hate speech – Commission initiative with social media platforms and civil society shows progress", European Commission, 1 June 2017, https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1471.

[66] ODIHR, "Hate Crime Data-Collection and Monitoring Mechanisms A Practical Guide", 2014, https://adsdatabase.ohchr.org/IssueLibrary/ODIHR_Practical%20guide%20-%20Hate%20crime%20data%20collection%20and%20monitoring.pdf.

groups facing gender-based threats in cyberspace, including journalists and those in public positions.[67]

Lastly, CSOs or society at large can also fuel the impetus for social media companies to improve solutioning to gendered threats. Since mid-2021, various prominent women leaders, public figures, and actresses have made calls to end online violence against women, some of which were directly addressed to the social media companies.[68] Hence, targeted and informed pressure coming from civil society may help push new initiatives in companies.

Conclusion

The pandemic has amplified online misogyny and hate speech in various parts of the world,[69] while disinformation and other online threats continue to be approached without much attention to gender. There is a need to better understand and raise awareness on structural problems concerning gender and security in online spaces while identifying contextual specificities. Future studies can explore the influence of differences in ICT infrastructure and cultural values on each country's priorities and their approaches to gender-based security in cyberspace.

We recommend that gender equality is supported by gender-focused policymaking in digital issues (such as cybersecurity, cyber safety, disinformation, and abuse), which recognises that there are different needs, risks, and impacts faced across different genders. We suggest that they seek gender-diverse multi-stakeholder views while building these policies. We finally recommend a multipronged approach and a cross border outlook to address these issues, acknowledging that the problem is not a women's issue alone and online violence knows no borders.

[67] Influenced by Lucina Di Meco's talk,18 May 2021, Nina Jankowicz, 18 May 2021, and Katharine M. Millar, 11 May 2021.

[68] Katie Collins, 1 July 2021; Alex Hern, 1 July 2021.

[69] "Social Media Monitoring on COVID-19 and Misogyny in Asia and the Pacific," UN Women, 2020, https://asiapacific.unwomen.org/en/digital-library/publications/2020/10/ap-social-media-monitoring-on-covid-19-and-misogyny-in-asia-and-the-pacific; Priyank Mathur, 25 May 2021

Acknowledgement

We would like to thank Benjamin Ang for sharing his views on some of the cybersecurity-related questions and providing feedback throughout the writing of this policy report. Also, we would like to reiterate that this policy report highlights and expands the discussions delivered in the three-part webinar series on "Gender, Security and Digital Space". Some of the points made by the speakers, which are summarised in the event report, are recapped in this piece for the substantial arguments to reach a wider audience. For more information on the webinar series and to access speakers' remarks, please refer to the event report (see footnote 1). An upcoming edited volume (Gulizar Haciyakupoglu, Yasmine Wong, and Benjamin Ang eds.) will explore urgent individual and national security questions concerning gender, security, and digital space.

About the Authors

Gulizar Haciyakupoglu is a Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Her research explores deliberate attempts of manipulation in information space, influence operations, and trust investment and activism in online platforms. Her recent publications appeared in various academic and policy outlets, including the Journal of Computer Mediated Communication, Defence Strategic Communications, The Diplomat, and The Interpreter. She holds a Ph.D. with Lee Kong Chian scholarship from the National University of Singapore (NUS), Communications and New Media Department (CNM), and an MA in Political Communication from the University of Sheffield. She received her bachelor's degree in Global and International Affairs from the Dual-Diploma Programme of the State University of New York (SUNY) Binghamton, and Bogazici University, Turkey.

Yasmine Wong is a Senior Analyst with the Centre of Excellence for National Security (CENS) of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Yasmine holds a Masters of Science in Political Sociology from the London School of Economics and Political Science. Her current research focuses on issues pertaining to social resilience, social cohesion and intergroup relations in both online and offline spaces.

About the Centre of Excellence for National Security (CENS)

The **S. Rajaratnam School of International Studies (RSIS)** is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

CENS is a research unit of RSIS at the Nanyang Technological University, Singapore. Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues. CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs.

For more details, please visit www.rsis.edu.sg and www.rsis.edu.sg/cens. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Nanyang Technological University, Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg