Global Network
on Extremism & Technology

A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism

Elsa Bengtsson Meuller

May 2023

GNET is a special project delivered by the International Centre for the Study of Radicalisation, King's College London.

The author of this report is
Elsa Bengtsson Meuller

The Global Network on Extremism and Technology (GNET) is an academic research initiative backed by the Global Internet Forum to Counter Terrorism (GIFCT), an independent but industry-funded initiative for better understanding, and counteracting, terrorist use of technology. GNET is convened and led by the International Centre for the Study of Radicalisation (ICSR), an academic research centre based within the Department of War Studies at King's College London. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing those, either expressed or implied, of GIFCT, GNET or ICSR.

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.

Recommended citation:
Bengtsson Meuller, Elsa. "A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism." London: Global Network on Extremism and Technology (GNET), May 2023. https://doi.org/10.18742/pub01-132.

Executive Summary

Online abuse and extremism disproportionately target marginalised populations, particularly people of colour, women and transgender and non-binary people. The core argument of this report focuses on the intersecting failure of Preventing and Counter Violent Extremism (P/CVE) policies and cybersecurity policies to centre the experiences and needs of victims and survivors of online extremism and abuse. In failing to do so, technology companies and states also fail to combat extremism.

The practice of online abuse is gendered and racialised in its design and works to assert dominance through male supremacist logic. Online abuse is often used by extremist groups such as the far right, jihadist groups and misogynist incels. Yet online abuse is not seen as a ‘threat of value’ in cybersecurity policies. Additionally, the discipline of terrorism studies has failed to engage with the intersection of racism and misogyny properly. Consequently, we fail to centre marginalised victims in our responses to extremism and abuse.

Through the implementation of a feminist theorisation of cybersecurity to tackle extremism, this report proposes three core shifts in our responses to online extremism:

1. Incorporate misogynist and racist online abuse into our conceptions of extremism.
2. Shift the focus from responding to attacks and violence to addressing structural violence online.
3. Empower and centre victims and survivors of online abuse and extremism.

The radical potential of this approach is that, while caring for victims, stakeholders also invest in developing responses that build stronger, supportive and educated counterforces to the abuse. When people receive help with the trauma experienced, individuals and communities are empowered to spot harms, help others and show a united front. Supportive and empowered communities help to ensure the upkeep of human rights. By bringing marginalised people’s experiences of violence into the centre of cybersecurity and P/CVE policies, we can impactfully redirect resources to create support mechanisms and initiatives that help victims of online violence and ultimately foster a community of care that challenges extremism and the structures of power that facilitate it. A feminist theorisation of cybersecurity can help us to tackle the roots of extremism.

Key findings

- Organisations currently fail to support the people who receive online abuse and violence. A victim-centred approach to tackling online violence, including that of online abuse and online extremism, in both cybersecurity and P/CVE policies is needed to enforce real change.

- Policymakers need to refocus and evaluate whether they put disproportionately more resources towards identifying perpetrators than helping victims and survivors of violence to work through their trauma.

- A theorisation of feminist cybersecurity centred on victims of online abuse and extremism can help to tackle extremist violence and work to counter the structures of power from which extremism stems.

- Misogynist and racist abuse online is both extreme and violent.

- Current P/CVE and cybersecurity areas' (including national policies) disengagement with gendered and racially oppressive structures means that strategies and activities that strive to counter extremisms are effectively built on male supremacist logic and consequently lack impactful intervention measures.

Contents

1 Introduction

Online abuse and extremism disproportionately target marginalised populations, particularly women and people of colour.[1] Perpetrators of online misogyny and racist abuse work to assert dominance through male supremacist logic and tactics, a practice often used by extremist groups such as the far right, jihadist groups and misogynist incels.[2] Lokmanoglu et al. found that the memes disseminated by extremist groups with the highest diffusion and virality had intersecting themes of gender and race.[3] However, the discipline of terrorism studies has failed properly to engage with the intersection of racism and misogyny in the assertion of fear and power.[4] It is imperative that our approach to countering extremism, both online and offline, recognises the ways in which online abuse plays out and reinforces extremist ideologies and practices, and how we fail to centre marginalised victims in our responses to extremism and abuse. By refocusing both Preventing and Counter Violent Extremism (P/CVE) policies and cybersecurity policies to centre victims of online abuse, we can start working on our biased practices and tackle the roots of extremism.

The core argument of this report focuses on the intersecting failure to centre the experiences and needs of victims and survivors of online extremism and abuse. In failing to do so, tech companies and states also fail to combat extremism. Through the implementation of a feminist theorisation of cybersecurity to tackle extremism, I propose three core shifts in our responses to online extremism: incorporate misogynist and racist online abuse as forms of extremisms, shift the focus from responding to attacks and violence to addressing structural violence online, and empower and centre victims and survivors of online abuse and extremism. We can challenge online violence by bringing marginalised people's experiences of violence into the centre of cybersecurity and P/CVE policies.[5]

Currently, P/CVE and cybersecurity policy frameworks do not recognise all the threats posed by (extremist) actors in cyberspace. This is due to a lack of reporting on cyberattacks, the connection of these cyberattacks to potential extremist actors and that traditional definitions of terrorism require violence to occur offline if it is to be

[1] Backe, Emma Louise, Pamela Lilleston, and Jennifer McCleary-Sills. 'Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence'. *Violence and Gender*, 2018.

[2] Roose, Joshua M., and Joana Cook. 'Supreme Men, Subjected Women: Gender Inequality and Violence in Jihadist, Far Right and Male Supremacist Ideologies'. *Studies in Conflict & Terrorism*, 2022: 1–29; Phelan, Alexandra, Jessica White, James Paterson, and Claudia Wallner. 'Misogyny and Masculinity: Toward a Typology of Gendered Narratives amongst the Far-Right'. Centre for Research and Evidence on Security Threats. https://crestresearch.ac.uk/comment/misogyny-and-masculinity-toward-a-typology-of-gendered-narratives-amongst-the-far-right/; Elizabeth Pearson et al., 'Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field' (VOX-Pol, 2023), https://www.voxpol.eu/download/report/Online-Extremism-and-Terrorism-Researchers-Security-Safety-Resilience.pdf.

[3] Lokmanoglu, Ayse, Allaham Mowafak, Abhari Rod, Chloe Mortenson, and Villa-Turek Esteban. 'A Picture Is Worth a Thousand (S)Words: Classification and Diffusion of Memes on a Partisan Media Platform'. GNET, 2023. https://gnet-research.org/2023/03/29/a-picture-is-worth-a-thousand-swords-classi%ef%ac%81cation-and-di%ef%ac%80usion-of-memes-on-a-partisan-media-platform/.

[4] Gentry, Caron E. 'Misogynistic Terrorism: It Has Always Been Here'. *Critical Studies on Terrorism* 15, no. 1 (2 January 2022): 209–24.

[5] Slupska, J. 'Safer (Cyber)Spaces: Reconfiguring Digital Security towards Solidarity'. 2022.; Iyer, Neema. 'Alternate Realities, Alternate Internets: African Feminist Research for a Feminist Internet'. In *The Palgrave Handbook of Gendered Violence and Technology*, edited by Anastasia Powell, Asher Flynn, and Lisa Sugiura, 93–113. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-83734-1_6.

incorporated into broader terrorism databases. In turn, our knowledge of the connection between traditional cyberthreats and extremism is undeveloped.[6] Of equal concern, as of the 2020s, the trends in identifying new 'threats' in cybersecurity are reinforcing gendered and racial structures of security and privilege.[7] These structures of security focus on national and corporate operational information defence and warfare,[8] through a masculinist and militarised lens, and centre on the protection of the state.[9] The result is that 'everyday' abuses in cyberspace, such as misogynist and racist abuse, are not being viewed as extreme enough to be incorporated into P/CVE policies. Consequently, the perpetrators of misogynist and racist abuse are not considered 'threats of value' in cybersecurity policies.

A theorisation of feminist cybersecurity centred on victims of online abuse and extremism can help us both to tackle extremist violence and to work to counter the structures of power from which extremism stems. The relative lack of engagement with gendered and racially oppressive structures by many currently working in the P/CVE and cybersecurity fields means that strategies and activities created to counter extremisms built on, for example, male supremacist logic lack impactful interventions.[10] Subsequently, we need to refocus our policies and evaluate whether we put disproportionately more resources into identifying perpetrators rather than supporting victims and survivors of this violence. If we do not centre victims in our responses to extremism, we are as accountable to the harm of this violence as the perpetrators.[11]

This report explores the following questions: What does it mean to adopt a feminist approach to cybersecurity and extremism? How do perceptions of gender influence the way we approach online abuse and extremism? This report introduces a theoretical framework of feminist cybersecurity. I explore how the adoption of a feminist cybersecurity approach to identify and counter violent extremism can serve to challenge the marginalisation of voices and to counter extremism by centring the people who are most affected. In turn, this approach helps to tackle the structural roots of extremism. While the literature on feminist approaches to cybersecurity remains scarce,[12] relating

[6] Holt, Thomas J., Steven M. Chermak, Joshua D. Freilich, Noah Turner, and Emily Greene-Colozzi. 'Introducing and Exploring the Extremist Cybercrime Database (ECCD)'. *Crime & Delinquency*, 2022: 2

[7] Dunn Cavelty, Myriam. 'Cyber-Security'. In *The Routledge Handbook of New Security Studies*, edited by Peter Burgess, 154–62. London: Routledge, 2012; Slupska, Julia, Scarlet Dawson Duckworth, and Gina Neff. 'Reconfigure: Feminist Action Research in Cybersecurity', 2021. https://www.oii.ox.ac.uk/news-events/reports/reconfigure-feminist-action-research-in-cybersecurity; True, Jacqui, and Sri Eddyono. 'Preventing Violent Extremism – What Has Gender Got to Do with It? Gendered Perceptions and Roles in Indonesia'. *European Psychologist* 26, no. 1 (2021): 55–67.

[8] Sjoberg, Laura. 'Introduction to Security Studies: Feminist Contributions'. *Security Studies* 18, no. 2 (2009): 183–213.

[9] Brown, Deborah, and Allison Pytlak. 'Why Gender Matters in International Cyber Security | Association for Progressive Communications'. 2020. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security.

[10] White, Jessica. 'Finding the Right Mix: Re-Evaluating the Road to Gender-Equality in Countering Violent Extremism Programming'. *Critical Studies on Terrorism* 15, no. 3 (2022): 585–609; Agius, Christine, Alexandra Edney-Browne, Lucy Nicholas, and Kay Cook. 'Anti-Feminism, Gender and the Far-Right Gap in C/PVE Measures'. *Critical Studies on Terrorism* 15, no. 3 (2022): 681–705.

[11] Phadke, Shruti, Jessie Seiler, Tanushree Mitra, Kiran Garimella, Matthew Costello, and James Hawdon. 'Addressing Challenges and Opportunities in Online Extremism Research: An Interdisciplinary Perspective'. In *Companion Publication of the 2021 Conference on Computer Supported Cooperative Work and Social Computing*, 356–59. CSCW '21. New York, NY, USA: Association for Computing Machinery, 2021: 358

[12] Brown & Pytlak. 'Why Gender Matters in International Cyber Security'; Millar, Katharine, James Shires, and Tatiana Tropina. 'Gender Approaches to Cybersecurity'. UNIDIR, 2021. https://unidir.org/publication/gender-approaches-cybersecurity; Mhajne, Anwar, Luna K. C., and Crystal Whetstone. 'A Call for Feminist Analysis in Cybersecurity: Highlighting the Relevance of the Women, Peace and Security Agenda'. *LSE Women, Peace and Security Blog* (blog), 17 September 2021. https://blogs.lse.ac.uk/wps/2021/09/17/a-call-for-feminist-analysis-in-cybersecurity-highlighting-the-relevance-of-the-women-peace-and-security-agenda/; Slupska, Julia, Toby Shulruff, and Tara Hairston. 'Cybersecurity Must Learn from and Support Advocates Tackling Online Gender-Based Violence'. UNIDIR, 2021. https://www.unidir.org/commentary/cybersecurity-online-GBV.

literature on technology-facilitated abuse (tech abuse),[13] feminist internet studies,[14] feminist approaches to the study of extremism,[15] as well as Black feminist and decolonial theory,[16, 17] form an important base to understand the effects of online extremism and the structural forms of oppression from which this stems. This report acknowledges the harm online extremist cultures cause to people online, but also how it affects one's life offline.

This report makes two core contributions to the field. First, I examine how a feminist theorisation of cybersecurity, theoretically and practically, can help us to understand the effects of online (and offline) violent extremism. This includes recognising that misogynist and racist abuse online is both extreme and violent. Second, I encourage a victim-centred approach to tackling online violence, including that of online abuse and online extremism, in both cybersecurity and P/CVE policies. This includes providing strategies for social media platforms on how to centre and empower victims and survivors of online extremism. Consequently, I demonstrate how we can better interrogate our responses to online extremism by illustrating how we currently fail to support the people who receive online abuse and violence.

This report speaks to GNET's commitment to applying a gender perspective to terrorist and violent extremist behaviour on digital platforms. The report is structured as follows. I begin by outlining the methodology adopted in this study. I then provide a brief literature review of feminist and gendered approaches to the study of extremism and a feminist critique of mainstream approaches to cybersecurity. The literature review is followed by my theoretical framework of feminist cybersecurity. In this section, I explore the framework by elaborating on the three shifts of focus: incorporating misogynist and racist online abuse as forms of extremism, changing focus from attack to structure, and centring victims as online P/CVE strategy. This is followed by a section on existing models of practice. I end this report emphasising the ways in which a feminist theorisation of cybersecurity can help us to tackle online extremism.

[13] Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock, and Bridget Harris. 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms'. *Feminist Media Studies* 18, no. 4 (4 July 2018): 609–25; Fiolet, Renee, Cynthia Brown, Molly Wellington, Karen Bentley, and Kelsey Hegarty. 'Exploring the Impact of Technology-Facilitated Abuse and Its Relationship with Domestic Violence: A Qualitative Study on Experts' Perceptions'. *Global Qualitative Nursing Research* 8 (2021); Tanczer, Leonie Maria, Isabel López-Neira, and Simon Parkin. '"I Feel like We're Really behind the Game": Perspectives of the United Kingdom's Intimate Partner Violence Support Sector on the Rise of Technology-Facilitated Abuse'. *Journal of Gender-Based Violence* 5, no. 3 (2021): 431–50.

[14] Iyer, 'Alternate Realities, Alternate Internets', 2021.

[15] Auchter, Jessica. *The Personal Is Political: Feminist Critiques of Countering Violent Extremism. Encountering Extremism*. Manchester University Press, 2020; Brown, Katherine E. 'Feminist Responses to Violent Extremism'. In *Routledge Handbook of Feminist Peace Research*. Routledge, 2021; Nwangwu, Chikodiri, Freedom C. Onuoha, Gerald E. Ezirim, and Kelechi C. Iwuamadi. 'Women, Intelligence Gathering and Countering Violent Extremism in Nigeria: A Postcolonial Feminist Discourse'. *Democracy and Security* 17, no. 3 (2021): 278–95.

[16] hooks, bell. *Feminism Is for Everybody: Passionate Politics*. 2nd ed. New York: Routledge, 2014; Hill Collins, Patricia. *Black Feminist Thought: Knowledge, Consciousness, and the Politics of Empowerment*. Vol. Rev. 10th anniversary ed. Perspectives on Gender. New York: Routledge, 2000.

[17] Tuhiwai Smith, Linda. *Decolonizing Methodologies Research and Indigenous Peoples*. 2nd ed. London: Zed Books, 2012.

2 Methodology

This report adopts an understanding of feminism that centres knowledge of Black and decolonial feminisms. Particularly, feminism in this report is seen as a political project that strives to eliminate gendered and sexist oppression,[18] a goal that is not possible without also eliminating intersecting systems of oppression, such as racism and cis-heteronormativity,[19] and recognising that the marginalisation of people is 'always embedded in histories of imperialism and colonisation'.[20] The struggle against systems of oppression needs to account for how forms of supremacism that maintain these systems are malleable and can change.[21] Part of this project is to centre marginalised processes of knowledge production, including that of using emotions as part of a methodology that interrogates whose feelings are acknowledged and valued. In turn, the interrogation of emotions reveals what we choose to see and make visible in political decisions and practices.[22] The theorisation of feminist cybersecurity to tackle extremisms needs to engage with how systems of power affect online abuse, which in turn affects (and works as a form of power for) victims and perpetrators of online violence.

To illustrate the applicability of a feminist approach to violent extremism, this report utilises the data gathered from twelve semi-structured interviews conducted with experts and professionals working in the tech, NGO and research sectors, as well as victims of online abuse. Sometimes these categories are overlapping. Eleven of the interviews were with women, one with a man. All interviewees are anonymised and their workplace is only specified, when necessary, superficially (for example, 'university', 'tech company', 'think tank', 'NGO').[23]

The report is also informed by first-hand data gathered from digital ethnographic methods. Specifically, the data used is from my notes, reflections and experience gathered during a one-year-long observational period of incels.is, a male supremacist and antifeminist online forum for misogynist incels. This data informs the ways in which vicarious trauma from reading and encountering hate and violence online affects observers; such effects have also been reported recently by Pearson et al.[24] and offline by Njoku.[25] In this report,

[18] hooks, *Feminism Is for Everybody*, 2014: xii

[19] Bey, Marquis. *Black Trans Feminism*. Durham: Duke University Press, 2022; Hill Collins, *Black Feminist Thought*, 2000; Lorde, Audre. *Your Silence Will Not Protect You*. London: Silver Press, 2017.

[20] Griffin, Penny, and Maryam Khalid. 'Gender, Race and Orientalism: The Governance of Terrorism and Violent Extremism in Global and Local Perspective'. *Critical Studies on Terrorism* 15, no. 3 (2022): 561.

[21] Carbado, Devon W., Kimberlé Williams Crenshaw, Vickie M. Mays, and Barbara Tomlinson. 'INTERSECTIONALITY: Mapping the Movements of a Theory'. *Du Bois Review: Social Science Research on Race* 10, no. 2 (2013): 303–12.

[22] Ahmed, Sara. *The Cultural Politics of Emotion*. Edinburgh: University Press, 2004; Tuhiwai Smith, *Decolonizing Methodologies*, 2012; Toyosaki, Satoshi. 'Toward De/Postcolonial Autoethnography: Critical Relationality With the Academic Second Persona'. *Cultural Studies ↔ Critical Methodologies* 18, no. 1 (2018): 32–42.

[23] The data collection conducted for this report has gone under ethics clearance and been approved by both Goldsmiths, University of London, and King's College, London.

[24] Pearson et al., 'Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field', 2023

[25] Njoku, Emeka Thaddues. 'The Ligaments of Counter-Terrorism Regime: Sexual Violence and the Vicarious Traumatisation of Female Non-Governmental Organisation Workers: Evidence from Nigeria'. *Small Wars & Insurgencies* 30, no. 6–7 (2019): 1,233–63.

the terms ‘online abuse’ and ‘online violence’ are intentionally broad in their application. While it is beyond the scope of this report to discuss what the concepts (should) encapsulate, online abuse should be seen as something in which both extremists and other people sometimes engage.

Limitations

There are two key limitations of this report. First, the limited number of interviews reflects the difficulty in finding participants to share their stories and experiences. A big challenge in this research was finding people who identified as victims or survivors of online abuse and who felt comfortable sharing their experiences. Additionally, it was difficult to recruit people from the tech sector who were willing to talk and share their expertise. While the number of interviewees is small, interviewees hold extensive experience working with or on the topic of online abuse and online violence. Second, most of my interviewees are based in the Global North, mainly Western Europe and the United States, and thus cannot speak for the Global South or specific countries. Overall, this report mainly draws on work situated in a Western context, with a few exceptions, which should be seen as a limitation of this study. The report should be seen as an inspiration for action that, in line with the feminist approach of the study, should be tailored to individual and community-specific circumstances.
I encourage using complementary context-specific resources to inform platform and national practices and policies when using a feminist approach to cybersecurity to tackle online extremism.

3 Feminist and Gender Approaches to Online Extremism

The application of gender approaches in the counterterrorism (CT) and P/CVE sectors, as well as in terrorism and extremism scholarship, have been marginalised in favour of masculinist approaches to security.[26] Terrorism and P/CVE literature experienced a boom after 9/11. This research was focused specifically on Islamist extremism, a focus that overshadowed the prominence of far-right extremists, which resulted in limited results in combatting extremist violence.[27] What is shared across both categories of extremism – far right and Islamist – is the lack of interrogation of the roles of gender and race.[28]

Agius et al. note how P/CVE efforts have failed to deal with anti-gender views and ideologies and subsequently failed to deal with sexism, misogyny, and transphobia.[29] When it comes to the engagement with gender in extremism and terrorism research, the norm has been to reinforce traditional, passive gender roles,[30] rid women of agency through victimisation,[31] and ignore the effect of gender dynamics when forming P/CVE practices and policies and in peace processes,[32, 33] as well as disregard how people involved in extremism reproduce and reinforce their group identity through gender norms.[34] Consequently, the literature on extremism and terrorism re-emphasises structural power and oppression by not critically investigating who is perpetrating violence and to whom this violence is directed.

Part of the issue of not engaging with wider societal power structures in the literature on extremism and terrorism is reflected in how we understand violence that is conducted online and its relationship to the ’offline world’. Research into tech abuse has shown that ‘technology has provided an opportunity for some to obtain power to exert greater control, monitor, stalk and harass their victims beyond the physical

[26] Agius, Christine, Alexandra Edney-Browne, Lucy Nicholas, and Kay Cook. ‘Anti-Feminism, Gender and the Far-Right Gap in C/PVE Measures’. *Critical Studies on Terrorism* 15, no. 3 (2022): 681–705; McCook, Sarah. ‘“So, What Is a Good Masculinity?”: Navigating Normativity in Violence Prevention with Men and Boys’. *Australian Feminist Studies* (2022): 1–17; Gentry, ‘Misogynistic Terrorism’, 2022.

[27] Rothermel, Ann-Kathrin. ‘Gender in the United Nations’ Agenda on Preventing and Countering Violent Extremism’. *International Feminist Journal of Politics* 22, no. 5 (2020): 720–41.

[28] Meier, Anna A. ‘Terror as Justice, Justice as Terror: Counterterrorism and Anti-Black Racism in the United States’. *Critical Studies on Terrorism* 15, no. 1 (2022): 83–101; Gentry, ‘Misogynistic Terrorism’ (2022): 209–24; Roose & Cook. ‘Supreme Men, Subjected Women’, (2022); Mondon, Aurelien. ‘Epistemologies of Ignorance in Far Right Studies: The Invisibilisation of Racism and Whiteness in Times of Populist Hype’. *Acta Politica*, 2022.

[29] Agius et al., ‘Anti-Feminism, Gender and the Far-Right Gap in C/PVE Measures’, 2022: 832–33.

[30] Patel, Sofia, and Jacqueline Westermann. ‘Women and Islamic-State Terrorism: An Assessment of How Gender Perspectives Are Integrated in Countering Violent Extremism Policy and Practices’. *Security Challenges* 14, no. 2 (2018): 53–83.

[31] Giscard d’Estaing, Sophie. ‘Engaging Women in Countering Violent Extremism: Avoiding Instrumentalisation and Furthering Agency’. *Gender & Development* 25, no. 1 (2017): 103–18.

[32] Asante, Doris, and Laura J. Shepherd. ‘Gender and Countering Violent Extremism in Women, Peace and Security National Action Plans’. *European Journal of Politics and Gender* 3, no. 3 (2020): 311–30.

[33] Parashar, Swati. ‘Gender, Jihad, and Jingoism: Women as Perpetrators, Planners, and Patrons of Militancy in Kashmir’. *Studies in Conflict & Terrorism* 34, no. 4 (2011): 295–317.

[34] Termeer, Agnes, and Isabelle Duyvesteyn. ‘The Inclusion of Women in Jihad: Gendered Practices of Legitimation in Islamic State Recruitment Propaganda’. *Critical Studies on Terrorism* 15, no. 2 (2022): 463–83.

space'.[35] While the issues of whether and how the internet plays a role in the ways in which extremists and others inflict harm has been of interest to scholars for some time,[36] the approach taken by states and tech companies to tackle these harms has been centred on a 'blame game'. Governments insinuate that tech companies do not do enough to tackle the harms perpetrated on their platforms. Tech companies in turn suggest that governments are not quick enough to offer practical guidelines on how to tackle the violence.[37] In the debate over who is responsible for making online platforms safe from extremist and harmful content, we have seen the concerning effects of the over-regulation of content by tech companies (for example, the deplatforming of marginalised content creators, such as sex workers)[38] to ensure that companies comply with national legislation or standards enforced by international regulatory bodies.[39] We have also seen concern expressed at how (liberal) governments are, due to their own disengagement, making tech companies sovereign entities with the power to regulate free speech.[40]

Using a feminist approach when investigating the internet-centred policies of states – particularly the trend in determining threats in states' cybersecurity and P/CVE policies and how this reflects tech companies' actions against online abuse – can help us to understand what is prioritised as a threat and what action to take when it comes to keeping cyberspace safe for marginalised people, such as women and people of colour. Literature on linking cybersecurity and P/CVE policies as a way to tackle online extremism is scarce;[41] a feminist or gender-focused approach is even more so. In the next section, I give an overview of traditional approaches to cyberthreats in cybersecurity policies. I provide a brief critique of the attribution of these threats and how this shows a disengagement with gender and race that affects marginalised people's security in cyberspace, before I introduce the feminist theorisation of cybersecurity and illustrate how P/CVE policies use similar biased practices of attribution to determine threats.

[35] Afrouz, Rojan. 'The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review'. *Trauma, Violence, & Abuse* 24, no. 2 (2023): 913–27.

[36] Conway, Maura. 'Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research'. *Studies in Conflict & Terrorism* 40, no. 1 (2017): 77–98; Winter, Charlie, Peter Neumann, Alexander Meleagrou-Hitchens, Magnus Ranstorp, Lorenzo Vidino, and Johanna Fürst. 'Online Extremism: Research Trends in Internet Activism, Radicalization, and Counter-Strategies'. *International Journal of Conflict and Violence*, 14 (2020): 1–20.

[37] Land, Molly K. 'Against Privatized Censorship: Proposals for Responsible Delegation'. *Virginia Journal of International Law* 60, no. 2 (2019): 363–432; Lewallen, Jonathan. 'Emerging Technologies and Problem Definition Uncertainty: The Case of Cybersecurity'. *Regulation & Governance* 15, no. 4 (2021): 1035–52.

[38] Are, Carolina, and Pam Briggs. 'The Emotional and Financial Impact of De-Platforming on Creators at the Margins'. *Social Media + Society* 9, no. 1 (2023).

[39] Chang, Brian. 'From Internet Referral Units to International Agreements; Censorship of the Internet by the UK and EU'. *Columbia Human Rights Law Review* 49, no. 2 (2017): 114–212.

[40] Land, 'Against Privatized Censorship', 2019.

[41] Holt et al., 'Introducing and Exploring the Extremist Cybercrime Database (ECCD)', 2022.

4 Bias in Cybersecurity: Missing Misogyny and Racism in the Attribution of Threats

The definition of 'cybersecurity' is in a state of some fluidity. The debate about the term circles around who or what is protected in cybersecurity practices.[42] Cybersecurity intends to protect the 'real cyber-geography' of cyberspace against potential threats to devices, data, information and software. A wider interpretation of cybersecurity would also describe it as the set of protocols, practices and technologies that are used to protect against perceived threats and insecurities apparent in and served through digital technology.[43] However, all types of threats that render cyberspace less secure for people are not accounted for in cybersecurity policies, such as tech abuse in intimate partner violence and the gendered and racialised workings of online abuse.[44, 45]

Concerns about security have traditionally been approached through a militarised lens and centred on the protection of the state.[46] Likewise approaches to cybersecurity have followed the same pattern.[47] The risk of attacks is usually the focus of national cybersecurity and foreign policies,[48] a pattern that also follows suit in corporate settings where ensuring the security of corporate information and data is prioritised.[49] Egloff and Dunn Cavelty argue that 'attribution' is key to understanding what is considered of political importance in cybersecurity. Attribution is the assessment of who is responsible for cybersecurity threats and what their intent was. Attribution therefore lays the foundations of a knowledge-creation process and reinforces cybersecurity standards and practices centred on attacks made by 'enemies'.[50]

Cybersecurity policies are malleable when it comes to recognising threats. While they tend to be formulated to address what are usually considered private matters and material,[51] national security and commercial interests can enforce or alter during attribution what

[42] Dunn Cavelty, 'Cyber-Security', 2012: 156.

[43] ibid.: 155–6.

[44] Slupska, Julia, and Leonie Maria Tanczer. 'Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things'. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, edited by Jane Bailey, Asher Flynn, and Nicola Henry. Emerald Studies In Digital Crime, Technology and Social Harms. Emerald Publishing Limited, 2021: 666

[45] Sharland, Lisa, Netta Goussac, Emilia Currey, Genevieve Feely, and Sarah O'Connor. 'System Update: Towards a Women, Peace and Cybersecurity Agenda'. UNIDIR. https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda: 36–7.

[46] Brown & Pytlak, 'Why Gender Matters in International Cyber Security', 2020: 3.

[47] Choucri, Nazli. *Cyberpolitics in International Relations*. The MIT Press, (2012): 5.

[48] Dunn Cavelty, 'Cyber-Security', 2012: 155–6.

[49] Slupska, Julia. 'Safe at Home: Towards a Feminist Critique of Cybersecurity'. SSRN Scholarly Paper. 2019; Shabut, Antesar M., K. T. Lwin, and M. A. Hossain. 'Cyber Attacks, Countermeasures, and Protection Schemes – A State of the Art Survey'. In *2016 10th International Conference on Software, Knowledge, Information Management & Applications (SKIMA)*, 37–44, 2016.

[50] Egloff, Florian J., and Myriam Dunn Cavelty. 'Attribution and Knowledge Creation Assemblages in Cybersecurity Politics'. *Journal of Cybersecurity* 7, no. 1 (2021): 1–2.

[51] Pierce, James, Sarah Fox, Nick Merrill, and Richmond Wong. 'Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity'. *Proceedings of the ACM on Human-Computer Interaction* 2, no. CSCW (2018): 1–24: 2–3.

is deemed to be a private or public matter.[52] For example, TikTok has been the subject of debate in the United States and elsewhere: the platform is mostly used by individuals sharing their content and information but there have been suspicions of surveillance via the app, which is Chinese-owned, by the Chinese state, which has caused some Western states to take actions to ban it, due to national security concerns.[53] What on the surface seems a matter of individuals' rights quickly falls under the purview of states' interests. Investigating attribution as a process of making a threat 'visible' through assigning the threat a traditional role as an (public) 'enemy' in security practices can help us to understand where governments and corporate actors assign 'threats of value'.[54] Attribution also tells us what are not considered meaningful threats. One area in which we can see a bias in the attribution of threats is when we consider online abuse, which disproportionately affects women and people of colour.[55] The lack of response by governments and tech companies illustrates how this is in no way a priority for them.

Noticeably, by deprioritising online abuse from mainstream cybersecurity policies, the attribution of threats in cyberspace is rendered a biased process. We see this in the traditional framing of cyber-threats, which centres the protection of the state, for instance at times when private matters become a public concern if the power of the state is threatened. The attribution of threats therefore reinforces an othering narrative by creating an enemy, or perpetrator, to the state (or corporation); the use of othering reinforces structural power.[56] It does so through a gendered and racialised imperial logic of protection in which those with the most power (for example, tech companies and states) can choose who to protect (the ones worthy of protection, the 'civilisable') and what or whom they protect you from ('the Other', the enemy).[57] As such, the attribution process in cybersecurity, just as in traditional P/CVE policies, can reinforce the role of the imperial and patriarchal protector – and does so currently by ignoring many of the actual victims of cyberthreats and harm.[58] The attribution of threats fails to care for victims and survivors of online misogynist and racist abuse by not providing impactful support to deal with their trauma, which reinforces white and male supremacism that nourishes extremist groups and ideologies. To address ignorance of gender and race in traditional cybersecurity policies, I propose a feminist theorisation of cybersecurity that centres victims and survivors of online abuse. In turn, the centring of victims and survivors help us to care for victims and to tackle harmful structures of power. A feminist theorisation of cybersecurity is, therefore, a practice that should be included in and make more effective P/CVE strategies. In the following sections of this report, I introduce and develop my proposed theoretical framework of feminist cybersecurity.

[52] Egloff & Dunn Cavelty, 'Attribution and Knowledge Creation Assemblages in Cybersecurity Politics', 2021: 3–4; Pierce et al., 'Differential Vulnerabilities and a Diversity of Tactics', 2018: 2–3.

[53] Kelly, Makena. 'Inside the US Government's Fight to Ban TikTok'. The Verge, 14 April 2023. https://www.theverge.com/2023/4/14/23682385/tiktok-ban-restrict-act-bytedance-china-free-speech.

[54] Dunn Cavelty, 'Cyber-Security', 2010: 62.

[55] Mhajne et al., 'A Call for Feminist Analysis in Cybersecurity', 2021.

[56] Dunn Cavelty, 'Cyber-Security', 2012: 162; Brown & Pytlak, 'Why Gender Matters in International Cyber Security', 2020.

[57] cooke, miriam. 'Gender and September 11: A Roundtable: Saving Brown Women'. *Signs: Journal of Women in Culture and Society* 28, no. 1 (2002): 468–70.

[58] Crawley, Heaven. 'Saving Brown Women from Brown Men? "Refugee Women", Gender and the Racialised Politics of Protection'. *Refugee Survey Quarterly* 41, no. 3 (2022): 355–80: 357.

5 A Feminist Theorisation of Cybersecurity to Tackle Online Extremism

There is a clear desire among policymakers to combat online abuse, such as racism and misogyny, but there is, seemingly, a lack of will to change the ways in which we prioritise misogyny and other online abuse. We have recently seen a decline in human and women's rights that directly affects women's and LGBTQIA+ safety in (cyber)spaces, such as attacks against the right to abortion in the USA,[59] the bodily autonomy of transgender individuals in the USA and UK,[60] and migrants' right to seek asylum in the UK.[61] We have also seen cyberspace used to intensify the conflict in Myanmar through online harassment and image-based abuse.[62] To challenge violence online, we need to do better at recognising how these abuses link to structural conditions of oppression and their extremist portrayals, including the mainstreaming of (particularly white and male) extremist ideas in public decision-making and discourse[63] – and how this affects who is considered an 'extremist' and, relatedly, what 'extremism' is.[64]

Extremist content is widely shared online, which has led to efforts by social media platforms to remove this material. The action to remove potentially harmful content online by social media companies has stemmed from the realisation that hosting this content facilitates extremist recruitment and radicalisation, and that tech companies 'now face potential regulatory repercussions for hosting such material'.[65] However, censorship via the law and tech company actions does not fully eliminate the problem of extremism or the root cause of extremist ideologies, if such attempts are not accompanied or driven by a commitment to structural changes.[66] For example, takedowns of both male supremacist and Islamic State accounts and platforms have led to a migration to other, in some cases more secure, anonymous social media and online sharing platforms and services.[67] I suggest that the continued existence of online practices of extremism indicates a failure to deal with the structural mechanisms that keep extremist ideologies

[59] Totenberg, Nina, and Sarah McCammon. 'Supreme Court Overturns Roe v. Wade, Ending Right to Abortion Upheld for Decades'. *NPR*, 24 June 2022. https://www.npr.org/2022/06/24/1102305878/supreme-court-abortion-roe-v-wade-decision-overturn.

[60] Savin, Jennifer. 'The Legal Definition of "sex" Could Soon Be Changed by the UK's Equality Minister'. Cosmopolitan, 5 April 2023. https://www.cosmopolitan.com/uk/reports/a43515648/definition-sex-changing/; Alfonseca, Kiara. 'Missouri to Implement Transgender Health Care Limitations for Adults, Minors'. ABC News. https://abcnews.go.com/US/missouri-implement-transgender-health-care-limitations-adults-minors/story?id=98584497.

[61] Scott, Jennifer. 'MPs Debating Illegal Migration Bill Clash as Tory Criticises "swarm" of Arrivals'. Sky News. https://news.sky.com/story/mps-debating-illegal-migration-bill-clash-as-tory-criticises-swarm-of-arrivals-12843686.

[62] Mhajne et al., 'A Call for Feminist Analysis in Cybersecurity', 2021.

[63] Brown, Katy, Aurelien Mondon, and Aaron Winter. 'The Far Right, the Mainstream and Mainstreaming: Towards a Heuristic Framework'. *Journal of Political Ideologies* (2021): 1–18.

[64] Mondon, Aurelien, and Aaron Winter. 'Racist Movements, the Far Right and Mainstreaming'. In *Routledge International Handbook of Contemporary Racisms*. Routledge, 2020: 149.

[65] McMinimy, Kayla, Carol K. Winkler, Ayse Deniz Lokmanoglu, and Monerah Almahmoud. 'Censoring Extremism: Influence of Online Restriction on Official Media Products of ISIS'. *Terrorism and Political Violence* (2021): 1–17: 1.

[66] Ebner, Julia. *Going Dark: The Secret Social Lives of Extremists*. London: Bloomsbury Publishing, 2020: 6.

[67] McMinimy et al., 'Censoring Extremism' (2021): 2; Bates, Laura. *Men Who Hate Women: The Extremism Nobody Is Talking About*. London: Simon & Schuster UK Ltd., 2020: 31.

alive. I argue that a feminist theorisation of cybersecurity can help us to deal with the roots of extremisms by adjusting our focus on fighting structures by centring victims of online abuse in our responses.

What would a feminist theorisation of cybersecurity look like? At root, I am proposing three core shifts in our understanding of online violence: reframing online abuse as part of the extremism spectrum; moving the focus in cybersecurity from responding to attacks and violence to addressing structural violence online; and centring victims as a core tenet of P/CVE and cybersecurity policies. Consequently, we need to realise that collaborating across policy areas is imperative to tackling online harms. A feminist theorisation of cybersecurity is different from a mere gendered approach to cybersecurity or P/CVE. It is not just interested in increasing the number of women in the workforce and the benefit to the organisation and / or national security that this brings, as identified by reports on gender and cybersecurity;[68] such a theorisation also affects change in the way that we think about being secure and safe in cyberspace and also critically examines how technology and the users of technology affect and are affected by cyberspace and who are prioritised in rendering cyberspace secure and safe. As such, 'a feminist approach to cybersecurity must be grounded by a focus on harms to people (particularly marginalised people) rather than devices or systems'.[69] Such an approach acknowledges that this abuse is currently an everyday phenomenon (for some more than others). When it comes to countering violent practices, simply applying the traditional sense and usage of securitisation – as has been done in mainstream cybersecurity policies – can lead to similarly violent or harmful outcomes.[70]

In turn, applying a feminist approach to cybersecurity in particular, and security in general, needs to be examined and tried for its biases and possible harmful effects if we are to use it in P/CVE. By applying a mere discursive practice of feminism in a security context we may risk it becoming co-opted by antifeminist forces and practices.[71] Therefore it is necessary to consider how security practices can be moved away from the ways which have resulted in failure in the past. We need to move away from mainstream practices of security that marginalise victims of online abuse if we are serious about challenging harmful and extremist content and actors.

Incorporating Gendered and Racist Online Abuse into Conceptions of Extremism

This report emphasises the need to consider online abuse as part of the spectrum of extremism. The use of the internet to create insecurity and fear is an intentional act that reinforces supremacist structures.[72] The intersection of online abuse and extremism is well documented; online abuse forms a core part of extremist practices, as a direct action.[73] This online abuse then often translates into real-world

[68] Kshetri, Nir, and Maya Chhetri. 'Gender Asymmetry in Cybersecurity: Socioeconomic Causes and Consequences'. *Computer* 55, no. 2 (2022): 72–77.

[69] Slupska, 'Safer (Cyber)Spaces', 2022: 17.

[70] Sjoberg, Laura. 'What, and Where, Is Feminist Security Studies?' *Journal of Regional Security* 11, no. 2 (2016): 143–61.

[71] ibid., 144.

[72] Pain, Rachel. 'Everyday Terrorism: Connecting Domestic Violence and Global Terrorism'. *Progress in Human Geography* 38, no. 4 (2014): 531–50.

[73] Díaz, Pablo Castillo, and Nahla Valji. 'Symbiosis of Misogyny and Violent Extremism: New Understandings and Policy Implications'. *Journal of International Affairs* 72, no. 2 (2019): 37–56: 41.

targeting. For example, reported jihadist extremist attacks are followed by spikes of anti-Muslim hate expressed both online and offline.[74] Online abuse also affects its audience through exposure to extremist, harmful, content.[75] This exposure can also occur through engaging with 'secondary abuse' by way of sharing violent and extremist memes,[76] through disseminating racist and misogynist memes,[77] or through researching extremism.[78] Part of the problem with current practices within cybersecurity policies is the lack of recognition of the physical, psychological and emotional impacts that abuse and violence conducted online have on the people who are exposed to, receive or are targeted with them.[79] The impact of online abuse works similarly to that of domestic violence, creating a culture of fear that can be seen as a form of 'everyday' terrorism.[80]

Currently, responses to online abuse fail to recognise who tends to be targeted by extremist actors: women, people of colour, and trans and non-binary people.[81] Misogyny and hostile sexism have been shown to be 'the factors most strongly associated with support for violent extremism'.[82] Actors of the Manosphere, who carry out much of their violence online, as well as racist actors protected under white supremacist structures (such as by invoking the First Amendment in the United States to protect themselves against charges of hate crimes) are asserting practices of supremacy.[83] Misogyny and racism as core facets of terrorism and extremism should, therefore, be centred in P/CVE responses. If we were to address gender-based hate and racism online, we would address a core facet of extremism.

Transition from Attack Focus to Structural Focus

P/CVE efforts and cybersecurity practices tend to focus on individual attacks rather than the structural reasons for (extremist) violence. The focus on attacks is enforced though the process of threat attribution that individualises the source of the violence. For example, current P/CVE efforts into antifeminist and antigender extremism have tended to focus on the violence committed, rather than the ideology behind such attacks.[84] Using attribution as an approach, we fail to examine the failures inherent in preventing and tackling online and offline extremist violence in this way, particularly the failure to address the structural sources of violence.

[74] Feldman, Matthew, and Mark Littler. 'Tell MAMA Reporting 2013/14: Anti-Muslim Overview, Analysis and "Cumulative Extremism"', 2014. https://www.tellmamauk.org/wp-content/uploads/2014/07/finalreport.pdf.

[75] Pearson et al., 'Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field', 2023: 54

[76] Crawford, Blyth, Florence Keen, and Guillermo Suarez-Tangil. 'Memes, Radicalisation, and the Promotion of Violence on Chan Sites'. *Proceedings of the International AAAI Conference on Web and Social Media* 15 (22 May 2021): 982–91.

[77] Lokmanoglu et al., 'A Picture Is Worth a Thousand (S)Words', 2023.

[78] Pearson et al., 'Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field', 2023: 54

[79] Alichie, Bridget. '"You Don't Talk like a Woman": The Influence of Gender Identity in the Constructions of Online Misogyny'. *Feminist Media Studies*, (2022): 1–20; Dragiewicz, Molly, Jean Burgess, Ariadna Matamoros-Fernández, Michael Salter, Nicolas P. Suzor, Delanie Woodlock, and Bridget Harris. 'Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms'. *Feminist Media Studies* 18, no. 4 (2018): 609–25: 619.

[80] Pain, 'Everyday Terrorism', 1 August 2014: 531–50.

[81] Backe, Emma Louise, Pamela Lilleston, and Jennifer McCleary-Sills. 'Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence'. *Violence and Gender* (2018).

[82] Johnston, Melissa, and Jacqui True. 'Misogyny & Violent Extremism: Implications for Preventing Violent Extremism', UN Women, 14 October 2019. https://research.monash.edu/en/publications/misogyny-amp-violent-extremism-implications-for-preventing-violen.

[83] The Institute for Strategic Dialogue. 'Andrew Tate's Misogynistic Views Aren't Unique, but Are Part of a Bigger Trend'. ISD. https://www.isdglobal.org/isd-in-the-news/andrew-tates-misogynistic-views-arent-unique-but-are-part-of-a-bigger-trend-online/.; Bell, Jeannine. 'There Are No Racists Here: The Rise of Racial Extremism, When No One Is Racist'. *Michigan Journal of Race & Law* 20, no. 2 (2014): 349–76.

[84] Agius et al., 'Anti-Feminism, Gender and the Far-Right Gap in C/PVE Measures', 2022: 696.

The elimination of misogynist and racist online abuse will not happen by using mainstream approaches to cybersecurity and online-based P/CVE policies, such as by attributing misogynists and racists as individualised 'enemies'. The problem lies in the method. The attribution of threats has, historically, led to instances of assigning an individualised role of the enemy to something that or someone who stems from deeper structural conditions, while ignoring that very structure of power, which does not lead to long-term changes for those affected by the (threat of) violence.[85] The nature of online abuse is not an individualised phenomenon but a systematic and coordinated practice that stems from structural conditions of power.[86] To challenge threats in cyberspace, we need to make cyberspace a place where these techniques of systematic intimidation do not overwhelm us.

How we talk, write and make gender and race important or unimportant in policies on cybersecurity and extremism have a real-world impact on actors who engage in perpetrating or countering violence. This is because our understanding and assumptions of gender 'inform how policymakers attempt to counter terrorism, extremism and political violence. These assumptions therefore influence and shape the global governance of terrorism and violent extremism.'[87] Governments and tech companies have the ability to change their priorities. These actors can challenge the traditional approach of attributing violent actions to a clear 'enemy' in cyberspace to focusing on where the threat stems from: structural conditions. Structural violence can be enforced in everyday but harmful practices by people, such as gendered and racialised harassment against women in politics,[88] networked misogyny and misogynoir.[89, 90] By individualising the threat, we do not challenge the systems wherein the threat can flourish.[91]

Incorporating a feminist theorisation of cybersecurity to tackle extremism may contribute to holistic approaches to challenge the source of the violence, including removing violent actors (and material) from the online space by tackling structural conditions of power. To apply a feminist theorisation to cybersecurity to tackle extremist violence adequately, we need to change the focus in the mainstream context: we need to move away from solely focusing on the 'attacks' and see the failures. To be able to see the failures, we need to move from thinking about cybersecurity as concerned solely with the protection of data to that of being safe as human beings online, protected from likely harms.[92] To acknowledge the parts of online violence that are currently not present in internet-centred policies starts with including these issues in the theorisation and practices of cybersecurity and P/CVE policies. We can do so by recognising the psychological and emotional effects and harm of online abuse, particularly how this abuse is extreme and often takes the form of misogyny and racism.

[85] Dunn Cavelty, 'Cyber-Security', 2012: 162.

[86] Marwick, Alice E., and Robyn Caplan. 'Drinking Male Tears: Language, the Manosphere, and Networked Harassment'. *Feminist Media Studies* 18, no. 4 (4 July 2018): 543–59: 544.

[87] Rothermel, Ann-Kathrin, and Laura J. Shepherd. 'Introduction: Gender and the Governance of Terrorism and Violent Extremism'. *Critical Studies on Terrorism* 15, no. 3 (2022): 523.

[88] Harmer, Emily, and Rosalynd Southern. 'Digital Microaggressions and Everyday Othering: An Analysis of Tweets Sent to Women Members of Parliament in the UK'. *Information, Communication & Society* 24, no. 14 (2021): 1998–2015.

[89] Banet-Weiser, Sarah, and Kate M. Miltner. '#MasculinitySoFragile: Culture, Structure, and Networked Misogyny'. *Feminist Media Studies* 16, no. 1 (2016): 171–4.

[90] Lawson, Caitlin E. 'Platform Vulnerabilities: Harassment and Misogynoir in the Digital Attack on Leslie Jones'. *Information, Communication & Society* 21, no. 6 (2018): 818–33.

[91] Shepherd, Laura J. 'White Feminism and the Governance of Violent Extremism'. *Critical Studies on Terrorism* 15, no. 3 (2022): 727–49.

[92] Strohmayer, Angelika, Rosanna Bellini, and Julia Slupska. 'Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm from Security to Safety'. *IEEE Pervasive Computing* 21, no. 3 (2022): 61–69: 62.

Centring Victims as Part of Online P/CVE Strategy

Centring victims of online abuse and cyberviolence can be a radical methodological tool that identifies where we are failing as well as systematically challenging extremist and supremacist actors. In line with Slupska, I argue that this means that we need to reframe cybersecurity 'to make it more caring, and people-centred'.[93] To make cybersecurity more people-centred, we can start by focusing on people's suffering, such as the emotional and psychological harm they have experienced.[94] By bringing a safety-centred understanding to cybersecurity that centres victims and survivors, we can design support mechanisms that feel reliable to people who disproportionately become victims of online abuse and extremist actors.

Russell argues that bodies that cannot be defined through a white supremacist and patriarchal 'primary gaze' are pushed to the margins.[95] The identity that does not align smoothly with whiteness and maleness becomes 'flattened' and given less territory to explore, to be 'free', which decontextualises and depoliticises experiences of injustice.[96] I argue that the silencing factor of misogynist and racist abuse works to flatten marginalised peoples' existence in cyberspace, which reinforces structural conditions of power. The unobstructed opportunity to feel, transform and express oneself online is stripped away, which in turn affects how we see and value marginalised people's experiences online – and offline. Through flattening, bodies are rendered 'faceless and unrecognizable', which makes it easier 'to establish a position of supremacy over another'.[97]

The process of flattening identities and rendering some bodies more visible than others can also be seen in whose experiences of abuse are made visible (and, subsequently, which are rendered invisible) in governments' and tech companies' responses to violence. Flattening as a mechanism of establishing supremacy is seen in extremist actors and groups, such as misogynist incel communities, in how they dehumanise women by referring to them as 'holes', 'foids' (female humanoids, thus subhuman) and other derogatory terms.[98] But when we only focus on the perpetrators rather than the victims (as per traditional attribution processes), as the latest trends in research into the mental health of incels has particularly tended to do,[99] we render the perpetrators recognisable while the victims unrecognisable. By humanising, acknowledging and centring victims and survivors of online violence, we directly challenge and counter the supremacism exerted by people online and in perpetrator/enemy-centred P/CVE and cybersecurity policies. Depending on what measures we choose to emphasise in our struggle against extremisms and violence, we choose how we want the internet and, by extension, the offline realm to be.

[93] Slupska, 'Safer (Cyber)Spaces', 2022: 31.
[94] ibid.
[95] Russell, Legacy. *Glitch Feminism: A Manifesto*. London: Verso, 2020: 20-21.
[96] Crawley, 'Saving Brown Women from Brown Men?', 2022: 357.
[97] Russell, *Glitch Feminism*, 2020: 21.
[98] Kelly, Megan, Alex DiBranco, and Julia DeCook. 'Misogynist Incels and Male Supremacism'. New America, 18 February 2021. http://newamerica.org/political-reform/reports/misogynist-incels-and-male-supremacism/.
[99] Moskalenko, Sophia, Juncal Fernández-Garayzábal González, Naama Kates, and Jesse Morton. 'Incel Ideology, Radicalization and Mental Health: A Survey Study'. *The Journal of Intelligence, Conflict, and Warfare* 4, no. 3 (31 January 2022): 1–29.; Sparks, Brandon, Alexandra M. Zidenberg, and Mark E. Olver. 'Involuntary Celibacy: A Review of Incel Ideology and Experiences with Dating, Rejection, and Associated Mental Health and Emotional Sequelae'. *Current Psychiatry Reports* 24, no. 12 (1 December 2022): 731–40.

I argue that we need to acknowledge and recognise the value in redirecting resources to victim- and survivor-centred responses within sectors that are involved in countering extremisms, including states' P/CVE and cybersecurity policies, technology and social media companies' policies and those of non-governmental organisations. A holistic approach to countering (online) extremism and terrorism is to work to tackle the structural forms of power and oppressions that let them grow (and sometimes flourish). By centring our responses on survivors and victims, we will evidently centre the people who receive the abuse rather than directing resources to removing 'the bad apples'. This includes destigmatising the use of and investing in mental health services. Individualising threats do not tackle the structural mechanisms that feed extremism and terrorism nor help with the trauma and abuse already experienced by victims. The radical potential of this approach is that, while caring for victims, we also invest in developing responses that build stronger, supportive and educated counterforces against the abuse. When people receive help, they and their communities are empowered to spot harms, help others and present a united front against these harms. Supportive and empowered communities help to ensure the upkeep of human rights.

The focus on victims of online abuse necessarily makes us re-evaluate what is extreme. Considering the disproportionate abuse directed at women and people of colour, both misogyny and racism need to be considered as extreme violence that is perpetrated to reinforce structural oppression. As it stands now, abuse online is seen as an unavoidable 'everyday' practice in cyberspace.[100] We cannot let online abuse be an 'ignorable' instance of abuse, whether it is the space where the abuse is conducted that reinforces it or the type of abuse carried out. It is essential to work towards a safer online environment for marginalised people if we want both to eliminate extremist violence and to counter the structures of power from which extremism stems.[101] I argue that by centring care as the practice that will eliminate prejudiced violence, as emphasised in feminist practices,[102] we can work to build stronger cultures that counter the violence conducted online and encourage investment in adequate responses and support systems for victims of the abuse. Thus, when it comes to the study of extremisms and countering extremism practices, we need to collaborate over disciplinary and sector boundaries if we are interested in challenging and combating the root of the issue of extremism.[103]

[100] Sambasivan, Nithya, Amna Batool, Nova Ahmed, Tara Matthews, Kurt Thomas, Laura Sanely Gaytán-Lugo, David Nemer, Elie Bursztein, Elizabeth Churchill, and Sunny Consolvo. '"They Don't Leave Us Alone Anywhere We Go": Gender and Digital Abuse in South Asia'. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 1–14. CHI '19. New York, NY, USA: Association for Computing Machinery, 2019.

[101] Slupska, 'Safer (Cyber)Spaces', 2022; Iyer, 'Alternate Realities, Alternate Internets', 2021: 93–113.

[102] Hill Collins, *Black Feminist Thought*, 2000; hooks, *Feminism Is for Everybody*, 2014.

[103] Conway, 'Determining the Role of the Internet in Violent Extremism and Terrorism', 2017: 88.

6 Existing Models of Practice

Some tech companies have already implemented some measures to help victims and survivors, including signposting mental health resources and local women's shelters. While this is a step forwards, these policies are mostly a stance of 'ethics-washing': 'a performative display of interest in countering abuse without meaningful action'.[104] Currently, many tech companies' support services end after they have signposted someone to other organisations' resources or services. This approach both risks overloading these further services and dismissing a company's responsibility for the abuse committed on its platform. Furthermore, the services of signposting that do exist on tech companies' platforms are not as accessible as they could be. Accessibility could be increased by implementing a design that includes these features by default on one's home screen (with an easy 'exit' option for victims and survivors who are near their abuser and want to conceal what they had been looking at). Designing online platforms in a way that makes reporting and support services more accessible could help people to reach out and foster a community of care. Currently, on major social media platforms, the features available all rely on the user being knowledgeable either about what resources are available or how to search for them.

Governments and tech companies are lacking in their practices of support for victims and survivors of online abuse but there are several organisations already helping victims and survivors of online abuse that tech companies (and governments) can learn from. Chayn[105] and Glitch UK[106] centre marginalised people and identities in their practices to challenge online abuse and domestic violence. There are also organisations that focus on furthering equality, education about and the reach of the internet to marginalised people, such as the Association for Progressive Communications (APC),[107] and organisations that focus on extending knowledge of cyberspace and everyday cybersecurity to people, such as Tactical Tech,[108] and making knowledge about extremism accessible to neurodiverse individuals, such as Autism Against Fascism.[109] All these organisations and groups are at the forefront of how to deal with structural issues that exist and travel between our online and offline practices, including that of challenging sexism, misogyny, racism, ableism and Eurocentricity. In the area of countering extremism, we need to recognise and learn from these types of organisations to see how their expertise and services help the people most affected by online abuse, including the abuse stemming from extremism and terrorism – and interrogate the potentially harmful responses the P/CVE sector may reinforce if we have a one-size-fits-all approach to countering online extremism.

[104] Strohmayer et al., 'Safety as a Grand Challenge in Pervasive Computing', 2022: 67.
[105] "Chayn – Supporting Survivors of Abuse across Borders," accessed 15 May 2023, https://www.chayn.co/.
[106] "Glitch," Glitch, accessed 15 May 2023, https://glitchcharity.co.uk/.
[107] "Association for Progressive Communications," accessed 15 May 2023, https://www.apc.org/.
[108] "Tactical Tech," accessed 15 May 2023, https://tacticaltech.org/.
[109] "Autism Against Fascism," Autism Against Fascism, accessed 15 May 2023, https://autismagainstfascism.wordpress.com/.

7 Conclusion

Cybersecurity and P/CVE policies' disengagement with tackling online abuse facilitates threats to marginalised people in cyberspace. This is particularly concerning since online abuse is a practice used extensively by extremist actors and groups.[110] To tackle online extremism, we need to make three core shifts in our responses: acknowledge the extremism of misogynist and racist online abuse, shift the focus from responding to attacks and violence to addressing structural violence online and centre victims and survivors of online abuse and extremism in our responses. We can do this by applying an approach to online extremism and abuse that builds on a theorisation of feminist cybersecurity. A feminist approach works to affect change in the way in which we think about being safe in cyberspace,[111] interrogates who is prioritised in rendering cyberspace secure and safe and critically examines how technology and the users of technology affect and are affected by cyberspace. In this report, I link the failure to centre victims of online abuse in cybersecurity policies to the failure of the P/CVE sector and the discipline of terrorism studies to deal with (online) misogyny and racism.[112]

A feminist approach to cybersecurity to combat extremist practices needs to challenge current responses to extremism and cyber threats, such as how threats are attributed and the focus on 'attacks.' A feminist approach does this by focusing on how power asserts itself through societal structures, such as white supremacy and patriarchy. In this report, I argued that the attribution of threats works on an imperial and gendered logic that ascribes digital actors of power (such as states and tech companies) a status as protector of the protected (the ones worthy of protecting, the 'civilisable') from the perpetrator (the making of the enemy/the Other). I argue that to counter structures of power that maintain inequalities, we must centre victims and survivors of online abuse, such as women, transgender people, non-binary people and people of colour (people who tend already to be marginalised in society) to craft impactful solutions to online extremism and abuse. Consequently, I argue that there needs to be a joint effort in providing solutions to support survivors of online abuse. If these support mechanisms should be impactful, we must make sure that enough help is provided for victims and survivors to work through their trauma accessibly. Simply redirecting victims to resources, such as local shelters, is not enough. Tech companies and states need to take responsibility for the abuse they facilitate on their platforms and gadgets by actively supporting the organisations to which they redirect victims. Information of how to deal with online abuse and violence also needs to be made more accessible through platform design.

[110] Roose & Cook, 'Supreme Men, Subjected Women', 2022; Phelan et al., 'Misogyny and Masculinity', 2023; Pearson et al., 'Online Extremism and Terrorism Researchers' Security, Safety, and Resilience: Findings from the Field', 2023.

[111] Slupska, 'Safer (Cyber)Spaces', 2022: 17.

[112] Gentry, 'Misogynistic Terrorism', 2022; Agius et al., 'Anti-feminism, gender and the far-right gap in C/PVE measures', 2022.

The application of a feminist theorisation of cybersecurity emphasises the tailoring of responses and the need to address power structures by also focusing on how people, and in turn cyberspace, are heterogenous. Our responses need to acknowledge and be adapted to particular contexts. Simply engaging in a one-size-fits-all approach to abuse and extremism seriously underestimates how violence is perpetrated. To understand online abuse better, we can further feminist cybersecurity theory by applying it to more contexts, such as engaging with smaller tech platforms and Global South contexts, in our efforts to counter violence. Further research into victim-centred responses on online platforms is needed to build on this framework. To do this, a closer collaboration with government and tech company actors is needed and encouraged.

Policy Section

This policy section has been authored by Dr Nicola Mathieson, Research Director, at the Global Network for Extremism and Technology (GNET) at the International Centre for the Study of Radicalisation (ICSR) at King's College London. This section provides policy recommendations and is produced independently from the authors of this report. Recommendations do not necessarily represent the views of the authors.

This report proposes that using a feminist theorisation of cybersecurity can enhance P/CVE policies. Drawing on intersectional feminist theory, Bengtsson Meuller proposes three core shifts in our responses to online extremism: incorporating misogynist and racist online abuse into an understanding of the forms of extremism, shifting the focus from responding to attacks and violence to addressing structural drivers of violence online and empowering and centring victims and survivors of online abuse and extremism. The key findings of this report carry corresponding policy implications for technology companies and policymakers.

This policy section ensures that GNET reports provide actionable research outcomes that can inform and support technology companies and policymakers to identify and prevent extremist and terrorist exploitation of digital platforms. The policy section fulfils GIFCT's core pillar of learning to improve prevention and responses to terrorist and violent extremist attacks.

1. Technology Companies

This report has identified three core areas for action for tech companies:

- This report builds on the growing body of literature that identifies hate speech and online abuse, especially that which targets minority groups, as a part of the extremism spectrum. While governments and international bodies have shifted their attention to addressing the intersection of online extremism and gender-based violence, tech companies need to develop more rigorous approaches to incorporating online abuse against minority groups that acknowledge this relationship.

- This report proposes radical changes to the way in which tech companies and governments approach cybersecurity and P/CVE by centring the experiences of victims of extremism and abuse. This approach shifts P/CVE policies from reactive to violent content to actively rethinking the structural component of the online environment that allows violence. This report challenges tech companies to think deeply about their responsibility not only to remove violent and terrorist content from their platforms but how their platforms might reproduce the structural conditions that allows for abuse online.

- Although removing extremist content and limiting its spread is a core part of tech companies' work, more work could be done to support victims of online abuse that occurs on their platforms. Tech companies should work with support services to develop a robust policy for supporting targeted groups that go beyond referrals to services.

2. Policymakers

In addition to the report findings and their implications for technology companies, this report has also identified three core areas for action by policymakers:

- Governments and policymakers have increasingly recognised the importance of the intersection of gender-based and intersectional violence and extremism, especially in the online environment. This report challenges policymakers to shift the priorities of P/CVE policy not only to address tech-facilitated gender-based violence but to think about structural approaches and priorities of P/CVE policy more broadly. Misogynist and racist online abuse forms a fundamental component of online extremists' behaviour online and is shared across extremist ideologies. Despite this, combating online abuse does not form a part of governments' P/CVE policy.

- There is an opportunity for policy to take a more holistic approach to P/CVE. As noted in this report, drawing on feminist theorisations of cyberspace, policy could be more effective at preventing violent extremism by addressing the structural causes behind such violence. This approach would not only help to prevent violent extremism but would also bring services that support victims on online abuse and extremism within the remit of P/CVE budgets. Support services for victims, especially marginalised groups, of abuse of all kinds pales in comparison to state budgets for P/CVE policies. There is an opportunity for P/CVE funding both to address the immediate harms of online extremism and to invest in services that form an essential part of whole-of-society prevention work.

- At the recent Canada Centre 2023 Conference on Countering Radicalization to Violence, a session was dedicated to hearing the voices and perspectives of victims and survivors in harm prevention and response. This session positioned victims and survivors as expert witnesses in the field. This session – complementing the findings of this report – demonstrates the immense value in listening to, and actioning the recommendations of, victims and survivors for both prevention and response.

Global Network
on Extremism & Technology

CONTACT DETAILS

For questions, queries and additional copies of this report, please contact:

ICSR
King's College London
Strand
London WC2R 2LS
United Kingdom

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Like all other GNET publications, this report can be downloaded free of charge from the GNET website at www.gnet-research.org.