Research Paper

International Security Programme

May 2024

Gendered hate speech, data breach and state overreach

Identifying the connections between gendered cyber harms to shape better policy responses

James Shires, Bassant Hassib and Amrit Swali

CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Contents

	Summary	2
01	Introduction	4
02	Gender and international cybersecurity	7
03	Three kinds of gendered cyber harm	10
04	Cascading and compounding gendered cyber harms	17
05	Conclusion and recommendations	33
	About the authors	38
	Acknowledgments	39

Summary

- Cybersecurity is more inclusive, more resilient and more effective when it actively and deliberately considers the threats, risks and harms that all users might face when they interact with cyberspace and digital technologies. This means recognizing that different groups of people – depending on age, socio-economic status or gender, among many other factors – experience cyberspace, and harms in cyberspace, in different ways. This paper focuses on gendered cyber harms specifically.
- There are three main kinds of cyber harm that have different impacts depending on a person's gender: **hate speech** (often via online harassment and abuse) and other content-based harms such as disinformation; **data breach** (privacy violations through the hacking or leaking of personal or sensitive data); and **state overreach** (for example, cybercrime laws or other legislation reinforcing discriminatory gender norms online).
- Studies of these gendered cyber harms have so far overlooked how each kind of harm interacts with the others. Understanding the interactions between hate speech, data breach and state overreach will contribute to better policy responses that view cybersecurity holistically, incorporating offline gendered dynamics and concerns into assessments of security risks.
- This paper analyses the connections between gendered cyber harms in six countries: the US, Poland, Uganda, Indonesia, Egypt and Brazil. This does not mean that gendered cyber harms occur only in these six countries, or that the prevalence or severity of such harms is exceptional there: the selection of countries is designed to show that gendered cyber harms are happening worldwide, across varying social and political contexts.
- The paper argues that gendered cyber harms are *cascading* and *compounding*. They are cascading because one form of gendered cyber harm leads to another. They are compounding because such cascades increase the impact on the people affected. Simply put, harms give rise to deeper harms.
- Understanding gendered cyber harms in this way leads to an appreciation of how offline and online gendered harms interact and intersect, thus reinforcing one another. For example, cyber threats to LGBTIQ+ people and communities might be an early indicator of a wider shift in negative government policies and attitudes to diverse gender expression in general.

- By identifying and understanding the connections between gendered cyber harms, states can, through policy and practice, better counter and mitigate these harms. The paper therefore makes the following policy recommendations:
  - **Combine technical, social and individual factors when analysing cyber threat and risk.** All three factors facilitate gendered cyber harms and contribute to their impact, and so the analysis of cyber threat, risk and vulnerability should be equally significant.
  - **Prioritize the protection of at-risk, marginalized and minoritized groups so that their security is treated as seriously as that of other national security assets and interests.** In practice, this entails improving data protection, privacy rights and cyber hygiene for everyone, especially vulnerable and at-risk groups. While this is not a gender-specific recommendation, it advances gender equality indirectly by ensuring that protection of vulnerable and at-risk groups is a priority.
  - **Adopt a gender-sensitive and human-centred approach to cybersecurity and cybercrime policy, legislation and strategy.** Gender-sensitive policy and implementation help states to counter rather than (inadvertently) exacerbate or introduce new gendered harms.
  - **Increase knowledge and coordination across different agencies and organizations working on cyber.** To avoid contradictions in policy and practice, states should institutionalize coordination between organizations and teams working on technical cybercrime, cybercrime legislation, gender policy and measures to counter disinformation.

01 Introduction

While gender is far from the only social component of cybersecurity, it is a key factor in understanding why cybersecurity approaches work for some and not others.

Cybersecurity is social as well as technical. While cybersecurity at its core concerns the protection of information and communications technology (ICT) devices, networks and systems,[1] it is also about keeping ICT users safe in cyberspace from cybercrimes, data and privacy violations, harmful and abusive content, and the plethora of risks that have emerged as the world has digitally transformed.[2]

This means that cybersecurity needs to be approached in a broad, human-centred, way.[3] Rather than starting from a particular notion of what counts as a cyberattack or threat, and defining cybersecurity as the practice of defending against that attack or threat, cybersecurity should start with the question of what is required to make people safe, and feel that they are safe, in their digital interactions and lives. Other work has laid out arguments for a broader approach to cybersecurity – in general, and specifically from a gender perspective.[4] This paper builds on those arguments and explores some of the many overlaps between technical cybersecurity and cybersecurity more broadly.

---

1 As one of the authors of this paper has previously written, this core concept of cybersecurity can be understood as 'the prevention and mitigation of malicious interference with digital devices and networks'. Even then, it contains multiple interpretations. See Shires, J. (2019) 'Family Resemblance or Family Argument? Three Perspectives on Cybersecurity and their Interactions', *St Antony's International Review*, 15(1), pp. 18–36, https://www.jamesshires.com/_files/ugd/92024e_490b5e322e80499c9e024c4da63f1e37.pdf. At greater length, the US defines cybersecurity in the 2008 National Security Presidential Directive (NSPD-54) / Homeland Security Presidential Directive 23 (NSPD-23) as 'prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation'. Key points of continued debate and tension are around the definition of 'integrity' (which could include broad notions of trust and safety in the internet) and 'information contained therein'. See also National Cyber Security Centre (undated), 'What is cybersecurity', https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.
2 Stevens, T. (2023), *What is Cybersecurity For?* Bristol: Bristol University Press; pp. 4–5.
3 Deibert, R. J. (2018), 'Toward a Human-Centric Approach to Cybersecurity', *Ethics & International Affairs*, 32(4), pp. 411–24, https://doi.org/10.1017/S0892679418000618.
4 Millar, K., Shires, J. and Tropina, T. (2022), *Gender Equality, Cybersecurity, and Security Sector Governance*, Geneva: Geneva Centre for Security Governance (DCAF), https://www.dcaf.ch/gender-equality-cybersecurity-and-security-sector-governance; Slupska, J. (2019), 'Safe at Home: Towards a Feminist Critique of Cybersecurity', *St Antony's International Review*, 15(1), pp. 83–100.

Moreover, cybersecurity does not stay online: it has offline or physical elements and consequences, affecting states, organizations and individuals.[5] Cyber *insecurity* poses reputational risks, has financial consequences and implications, and can threaten livelihoods, violate human rights and endanger critical infrastructure. And it leads to cyber harms – the latter defined as effects that originate from or are exacerbated in cyberspace, causing 'the diminishing, damage, or destruction of areas of human value, especially the body, affective life, and community'.[6]

Cyber harms – and the digital vulnerabilities and risks that perpetuate these harms – differ based on an individual's gender and other intersecting identities.[7] Such gendered differences affect the way cybersecurity, understood broadly, is perceived, experienced and delivered.[8]

Understanding of gendered cyber harms has advanced significantly in recent years.[9] Research in this area has identified three main kinds of gendered cyber harm: hate speech (often via online harassment and abuse) and other content-based harms such as disinformation; data breach (privacy violations through hacking or leaking personal or sensitive data); and state overreach (e.g. cybercrime legislation reinforcing discriminatory gender norms).

Cybersecurity does not stay online: it has offline or physical elements and consequences, affecting states, organizations and individuals.

So far, both research and policy have tended to consider these three kinds of gendered cyber harms separately. Furthermore, these harms may not even be considered gendered *cyber* harms under a narrow definition of cybersecurity. This approach has allowed each type of gendered harm to be addressed specifically and appropriately, but the separation overlooks how each kind of gendered harm may interact with the others, and how they can be mutually reinforcing; for example, how gendered abuse on social media platforms may make an individual a target for hacks and leaks, and may even lead to prosecution of the victim under cybercrime laws. This research paper therefore considers the connections

---

5 We define cyber insecurity simply as the lack of cybersecurity. Some studies prefer to highlight the intertwined nature of the two concepts, foregrounding how *cybersecurity for some* always coexists with *cyber insecurity for others*. For a similar argument regarding cyber stability, see Chesney, R., Shires, J. and Smeets, M. (eds) (2023), *Cyberspace and Instability*, Edinburgh: Edinburgh University Press.
6 Egloff, F. J. and Shires, J. (2023), 'The better angels of our digital nature? Offensive cyber capabilities and state violence', *European Journal of International Security*, 8(1), pp. 130–49, https://doi.org/10.1017/eis.2021.20. See also Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S. and Upton, D. (2018), 'A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate', *Journal of Cybersecurity*, 4(1), pp. 1–15, https://doi.org/10.1093/cybsec/tyy006.
7 Pierce, J., Fox, S., Merrill, N. and Wong, R. (2018), 'Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity', *Proceedings of the ACM on Human-Computer Interaction*, 2(CSCW), pp. 1–24, https://doi.org/10.1145/3274408.
8 Lobato, L. C. and Gonzalez, C. (2020), 'Embodying the Web, recoding gender: How feminists are shaping progressive politics in Latin America', *First Monday*, 25(5), https://doi.org/10.5210/fm.v25i5.10129.
9 For an overview, see Millar, K., Shires, J. and Tropina, T. (2021), *Gender approaches to cybersecurity: design, defence and response*, Geneva: United Nations Institute for Disarmament Research, https://doi.org/10.37559/GEN/21/01.

between different kinds of gendered cyber harm, how thinking about these harms in a more holistic way can help mitigate them, and what states can and should do to address them.

The paper argues that gendered cyber harms are *cascading* and *compounding*. They are cascading because one form of gendered cyber harm leads to another. They are compounding because such cascades increase the impact on the individual or individuals. In short, harms give rise to deeper harms. Understanding gendered cyber harms as cascading and compounding allows for a more comprehensive appreciation of how offline and online gender harms interact, intersect and reinforce one another. This understanding broadens the landscape of responsibility for designing, delivering and assessing cybersecurity, contributing to better policymaking that views gendered cyber harms as part of a broader security challenge.

The next chapter briefly introduces the concept of gender and its relevance to international cybersecurity. Chapter 3 then reviews the literature on the three kinds of gendered cyber harm. Chapter 4 connects these three kinds of harm through illustrative examples of cascading and compounding gendered cyber harms, drawn from a range of political and social contexts worldwide. The concluding chapter includes a set of policy recommendations intended to encourage gender-sensitive[10] and gender-transformative (i.e. challenging harmful gender norms, roles and realities) policy and governance responses to cyber insecurity.

10 See Emerson-Keeler, E., Swali, A. and Naylor, E. (2023), *Integrating gender in cybercrime capacity-building: a toolkit*, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135515: 'Gender sensitivity refers to fairness in the treatment of people, with appropriate accommodations made for those who are historically disadvantaged or marginalized, and awareness of the inherent biases and stereotypes that manifest themselves as discrimination. When activities, policies and processes are 'gender-sensitive', it means that they intentionally treat people as equal and with respect, and address inequalities that derive from gender identity.'

02 Gender and international cybersecurity

The development of a secure, safe, responsible and peaceful cyberspace for all is a global endeavour and priority, with interlocking development and security implications. Understanding the gendered dimensions of cybersecurity, therefore, is a matter of international security.

The UN defines gender as 'the social attributes and opportunities associated with being male and female and the relationships between women and men and girls and boys, as well as the relations between women and those between men'.[11] While definitions of gender are fluid – and are sometimes contested or politicized in public debate[12] – it is commonly understood that gender is socially constructed, evolving over time and often mirroring entrenched power hierarchies and dynamics. Notably, the word 'gender' is not synonymous or interchangeable with 'women'.[13]

As a social structure, gender is a system of power that creates and reinforces norms – i.e. standards of behaviour deemed appropriate in a given context. Gender norms are usually binary, generating specific expectations for the behaviour of men and women. This gender binary has two related characteristics. First, it is hierarchical, placing one gender above another and valuing subtypes of masculinity and femininity differently, leading to unequal power, access and opportunity.[14] Second, it is exclusionary, repressing and marginalizing diverse

11 See, for instance, 'Office of the Special Advisor on Gender Issues and Advancement of Women (2001), 'Gender Mainstreaming: Strategy for Promoting Gender Equality', https://www.un.org/womenwatch/osagi/pdf/factsheet1.pdf.
12 In its resources on sex and gender, for instance, the Council of Europe observes: 'Gender is a 'heavy' word: politicians and public figures often use it with negative connotations, for example in referring to 'gender police', or to ideologies that 'threaten our kids''. See Council of Europe (2024), 'Gender Matters: Sex and gender', https://www.coe.int/en/web/gender-matters/sex-and-gender.
13 See also Emerson-Keeler, Swali and Naylor (2023), *Integrating gender in cybercrime capacity-building: a toolkit*.
14 This is one way of understanding the term 'patriarchy'.

gender identities that do not fit within the binary. State and other institutional systems incorporate and amplify gender norms for political and other reasons, creating and exacerbating gendered cyber harms.

Gender is intersectional. A term coined by Kimberlé Crenshaw, 'intersectionality' traces how gender interacts with race and other social categories and identities, and how forms of discrimination manifest around these intersections.[15] To give just one example of why this matters in cyberspace, a 2023 report on 'digital misogynoir' studied the dehumanization of Black women on social media, and found significantly more highly toxic posts about Black women than white women.[16] An intersectional gender analysis includes people of LGBTIQ+ identities.[17] This paper examines cyber harms to LGBTIQ+ communities as gendered cyber harms, focusing on their cascading and compounding connections.

State and other institutional systems incorporate and amplify gender norms for political and other reasons, creating and exacerbating gendered cyber harms.

Online, the presentation of gender identity is influenced and governed variously by individual preferences, community norms, platform requirements and national legislation. Inferences and assumptions about gender identity are central to gendered cyber harms, from social media hate speech to the impacts of a data breach.

If our starting concern is how safe people are – and feel they are – online, then anything that increases individual insecurity and exposure to cyber harm constitutes a cybersecurity issue. Thus, while some policy approaches exclude the social media harms considered under 'hate speech' in this paper from the scope of cybersecurity (preferring to describe them as issues of 'online safety' or similar),[18] a gender-focused analysis encourages viewing them as issues of human (in)security online – i.e. cybersecurity.[19] Similarly, gendered cyber harms straddle standard distinctions between cyber-dependent and cyber-enabled threats and risks in the cybersecurity community.[20]

---

15 Crenshaw, K. W. (1991), 'Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color', *Stanford Law Review,* 43(6), pp. 1241–99, https://doi.org/10.2307/1229039.
16 Glitch, UK (2023), *The Digital Misogynoir Report: Ending the dehumanising of Black women on social media*, https://glitchcharity.co.uk/wp-content/uploads/2023/07/Glitch-Misogynoir-Report_Final_18Jul_v5_Single-Pages.pdf. This study found that, of a total of 200,976 toxic posts about women, 154,373 were about women in general; 27,874 were about Black women; and 18,729 were about white women.
17 The term LGBTIQ+ denotes a variety of personal characteristics outside heteronormativity, incorporating aspects of both sexual orientation and gender identity. Gender-based approaches generally consider discrimination based on sexual orientation within their scope of analysis for two reasons: first, such discrimination is often based on gendered stereotypes of 'normal' behaviour; second, such discrimination intersects with gender identities, affecting people of different genders differently.
18 The UK's 2023 Online Safety Act, for instance, refers to offences that affect women and girls, and covers issues of harmful content, but does not mention or conceive of these issues from the perspective of cybersecurity. For the full text of the legislation, see https://www.legislation.gov.uk/ukpga/2023/50/enacted.
19 The exclusion of certain (often gendered) topics from the 'proper' scope of security is a pattern that repeats in many issue areas, not confined to cybersecurity.
20 McGuire, M. and Dowling, S. (2013), *Cyber crime: A review of the evidence*, Home Office Research Report 75, https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence.

Secure access to ICTs can advance gender equality by increasing access to services for marginalized communities and people for communication, education and economic purposes. If access to and dissemination of these technologies is not coupled with a gender-sensitive understanding of the harms, vulnerabilities and risks that can arise from their use, the vast empowerment potential of ICTs for individual, organizational and national growth and sustainable development is put at risk. Just as the international development field has successfully connected the rights and protection of women and girls to social and economic development, connecting gendered understandings of cyberspace to (failures of) cybersecurity can lead to better overall international security both within and beyond the cyberspace domain.

The Women, Peace and Security (WPS) agenda offers an established and internationally recognized foundation for this work.[21] As explained by Sharland et al., the WPS agenda seeks to ensure that 'lessons learned from traditional peace and security processes are incorporated for the benefit of a sustainable open, free and stable digital world'.[22] Aligning (international) cybersecurity with the WPS agenda helps to identify and counter underappreciated or unseen gendered harms, and also consider how all genders – not just women and girls – experience cybersecurity. Furthermore, by treating gender equality and empowerment, along with principles of fairness, equality, equity and stability, as key priorities, a gender-transformative approach to cybersecurity is also a means for advocating against the militarization of cyberspace in general and, consequently, working towards a more inclusive vision of cyber peace.[23]

---

21 Hofstetter, J.-S. and Pourmalek, P. (2023), *Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity*, Global Network of Women Peacebuilders and ICT4Peace Foundation, https://gnwp.org/gender-cybersecurity-through-women-peace-security.
22 Sharland, L. et al. (2021), *System Update: Towards a Women, Peace and Cybersecurity Agenda*, Geneva: United Nations Institute for Disarmament Research, https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda.
23 Bernarding, N. and Kobel, V. (2023), *Feminist Perspectives on the Militarisation of Cyberspace*, Berlin: Centre for Feminist Foreign Policy, https://centreforfeministforeignpolicy.org/wordpress/wp-content/uploads/2023/06/CFFP_Briefing_Cybersecurity_final.pdf.

03 Three kinds of gendered cyber harm

The literature on gender and cybersecurity has identified three kinds of cyber harm that have gendered dimensions, considered in turn below. These cyber harms are separate to those stemming from lack of access to the internet or digital technologies (the 'gender digital divide'), which are themselves exacerbated by internet shutdowns and other deliberate impediments to online inclusion.[24] They are also separate to the issue of unequal gender participation in cybersecurity governance and technical fields, which is both a distinct policy problem and an important factor facilitating the harms discussed here.

3.1 Hate speech

The first kind of gendered cyber harm involves gendered hate speech, online abuse and disinformation. These are overlapping but distinct phenomena, all related to online content. Gendered hate speech is offensive content that attacks or targets people based on their gender identity, typically through pejorative or discriminatory elements; for example, misogynistic hate speech expresses a hatred of women. Gendered online abuse is similarly targeted at individuals or groups based on their gender identity, but does not necessarily involve the explicit content elements of hate speech.[25] Gendered disinformation is the

24 Brown, D. and Pytlak, A. (2020), *Why Gender Matters in International Cybersecurity*, Women's International League for Peace and Freedom and Association for Progressive Communications, https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security.

25 This paper's definition of online abuse includes what Amnesty International terms 'problematic content' – i.e. content that is harmful or hurtful but that does not necessarily meet a social media platform's own threshold for 'abusive content'. Amnesty International (2018), 'Women abused on Twitter every 30 seconds – new study', press release, 18 December 2018, https://www.amnesty.org.uk/press-releases/women-abused-twitter-every-30-seconds-new-study.

deliberate spread of false information regarding gender issues, and can be part of hate speech and online abuse.[26] The internet makes such dissemination easier, wider and more harmful, with new digital tools such as generative AI only extending this trend.

While gendered harassment and abuse online affects many people, Brown and Esterhuysen note that human rights defenders, journalists and those in vulnerable or marginalized situations face increased risks and suffer greater consequences from gender-based threats and abuse.[27] Haciyakupoglu and Wong underline the dependence of gendered online abuse on the business models and algorithmic design of large social media platforms, including metrics of engagement and virality that favour offensive or polarizing content.[28] In contrast, content moderation is often inadequately resourced and restricted by geography or language, meaning that the incentive structure of the commercial environment is weighted against protection and care for those targeted.[29] The problem spreads beyond major platforms, with gendered harassment and abuse also widespread in multiplayer online games, web forums and private or semi-public messaging apps – where appropriate policies are even harder to introduce and monitor.[30]

Gendered hate speech has implications for international politics. In her then capacity as UN Special Rapporteur on violence against women, Dubravka Šimonović highlighted the links between online and offline violence against women in politics, emphasizing how 'violence against women in politics is often normalized and tolerated, especially in contexts where patriarchy is deeply embedded'.[31] Di Meco notes deliberate attempts, based on misogynistic tropes and stereotypes around gender roles, to discourage women from seeking political careers and derail public support for women politicians.[32] Judson et al. investigate the specific problem of 'state-aligned' gendered disinformation: disinformation created by, for, or in support of state actors for political purposes.[33] Such studies highlight a range of techniques used to discredit women in political debate, as well

---

26 Although this section focuses on literature concerning disinformation, misinformation (false content created and/or spread unintentionally) is an equally important issue. In practice, misinformation and disinformation are difficult to separate, and so we treat them together in the empirical analysis in Chapter 4, section 4.1.
27 Brown, D. and Esterhuysen, A. (2019), 'Why cybersecurity is a human rights issue, and it is time to start treating it like one', Association for Progressive Communications, 28 November 2019 (updated 28 April 2023), https://www.apc.org/en/node/35879. See also Posetti, J. et al. (2021), *The Chilling: Global trends in online violence against women journalists*, Research Discussion Paper, United Nations Educational, Scientific and Cultural Organization (UNESCO), https://en.unesco.org/publications/thechilling.
28 Haciyakupoglu, G. and Wong, Y. (2021), *Gender, Security and Digital Space: Issues, Policies, and the Way Forward*, Policy Report, Singapore: S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University (NTU), https://www.rsis.edu.sg/rsis-publication/cens/gender-security-and-digital-space-issues-policies-and-the-way-forward.
29 Di Meco, L. (2023), *Monetizing Misogyny: Gendered Disinformation and the Undermining of Women's Rights and Democracy Globally*, #ShePersisted, https://she-persisted.org/wp-content/uploads/2023/02/ShePersisted_MonetizingMisogyny.pdf.
30 Barker, K. and Jurasz, O. (2019), *Online Misogyny as Hate Crime: A Channel for Legal Regulation?* Abingdon and New York: Routledge.
31 Šimonović, D. for UN Women (2020), *Violence Against Women in Politics,* Expert paper prepared for the Sixty-fifth session of the Commission on the Status of Women (CSW 65), https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/SRVAW_VAW%20in%20Politics_EP9_EGMCSW65.pdf.
32 Di Meco, L. for UN Women (2020), *Online Threats to Women's Political Participation and The Need for a Multi-Stakeholder, Cohesive Approach to Address Them*, Expert paper prepared for the Sixty-fifth session of the Commission on the Status of Women (CSW 65), p. 4, https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf.
33 Judson, E. et al. (2020), *Engendering Hate: The contours of state-aligned gendered disinformation online*, London: Demos, https://demos.co.uk/research/engendering-hate-the-contours-of-state-aligned-gendered-disinformation-online.

as its intersectional dimensions.[34] One UK study found that Black and Asian women members of parliament were more likely to be subject to online abuse.[35] Research events at Chatham House have demonstrated the co-option of gender narratives in nationalist disinformation campaigns in Georgia and Ukraine.[36]

It should be noted that women, girls and LGBTIQ+ people are not the only victims of gendered hate speech.[37] Extremist content is a form of hate speech, relying on stereotypes to create, generalize and spread harmful messages, and often, but not always, inciting online and offline violence or hate crimes. Those radicalized by extremist content might themselves be victims of hate speech that relies on such (gendered) stereotypes. In closed or coded online communities, extremist content contributes to the radicalization of all people, especially men and boys. Misogynistic stereotypes permeate many extremist ideologies. In some cases, gendered hate speech is instrumental to a broader process of radicalization; in others, misogyny may be the starting point around which an extremist community forms. In addition to gendered hate speech online, the offline harms resulting from radicalization range from acts of doxxing (searching for and revealing another person's private or identifying information, such as their real name or place of residence) to recruitment to terrorist organizations or 'lone wolf' acts of violence.[38]

In some cases, gendered hate speech is instrumental to a broader process of radicalization; in others, misogyny may be the starting point around which an extremist community forms.

Overall, gendered hate speech, online abuse and disinformation are cybersecurity issues because they are harmful to an individual's sense of security and belonging in cyberspace. While gender is far from the only lens through which to analyse hate speech, it is a highly visible aspect of an individual's identity. This means that, for both targets and perpetrators, gender is a focal point for victimization or abuse at both individual and group levels. Furthermore, the issue of gendered hate speech reveals a wider tension in personal decision-making around, and platform moderation of, online content: how to reconcile hypervisibility in terms of profile (the increased scrutiny and exposure experienced by certain gender identities) and invisibility in terms of solutions (as content moderation fails to address the harms felt by specific communities). For some groups of people, such as women in politics,

---

34 Jankowicz, N. et al. (2021), *Malign Creativity: How Gender, Sex and Lies are Weaponized Against Women Online*, Washington, DC: Wilson Center, https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online.
35 Amnesty International UK (2017), 'Black and Asian women MPs abused more online', https://www.amnesty.org.uk/online-violence-women-mps.
36 See, for example, Chatham House (2021), 'Strengthening Georgia's resilience to disinformation and cyber threats', research event, https://chathamhouse.soutron.net/Portal/Public/en-GB/RecordView/Index/190945.
37 Shoker, S. (2021), *Making gender visible in digital ICTs and international security*, Report submitted to Global Affairs Canada for the UN Open-Ended Working Group (OEWG) on Cybersecurity, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.
38 Bosman, J., Taylor, K. and Arango, T. (2019), 'A Common Trait Among Mass Killers: Hatred Toward Women', *New York Times*, 10 August 2019, https://www.nytimes.com/2019/08/10/us/mass-shootings-misogyny-dayton.html.

security through obscurity is not an option because their work is, by its nature, highly visible. Finally, gendered hate speech and online abuse clearly reverberate offline, with real-world consequences and impacts.

3.2 Data breach

The second kind of gendered cyber harm involves privacy violations due to data misuse, leakage or exploitation by malicious actors. There are two key ways in which online privacy violations and the misuse of digital data by those who do not have a legal or ethical right to access that data have gendered impacts. The first is as part of 'technology-facilitated violence and abuse' or 'digital coercive control': the incorporation of digital devices and data into strategies and techniques of intimate partner violence, online and offline.[39] The clearest example is 'stalkerware' – i.e. spyware that can send almost all of a device's data remotely to an abuser.[40] Crucially, technology-facilitated abuse is not limited to mobile devices and computers. Internet of things (IoT) devices such as smart speakers or Bluetooth and Wi-Fi trackers have also been abused for purposes of coercive control.[41]

The other is through the rise of 'femtech' – i.e. personal digital devices or apps designed for women. The rapid growth of this sector means that information and data on women's health – including menstrual cycles, pregnancy, birth control and abortion – are increasingly vulnerable to cybersecurity vulnerabilities and risks, ranging from commercial de-anonymization to the publication and exploitation of leaked data. Recent studies highlight the gulf between the collection and use of data by femtech apps and devices, and users' understanding and sense of control of that data.[42] Harms stemming from data leakage range from psychological impacts of inappropriate advertising, for example increasing an individual's sense of violation and trauma after miscarriage,[43] to the physical and legal implications for people seeking abortions (discussed later in this paper). As these devices and

---

39 Harris, B. A. and Woodlock, D. (2019), 'Digital Coercive Control: Insights From Two Landmark Domestic Violence Studies', *The British Journal of Criminology*, 59(3), pp. 530–50, https://doi.org/10.1093/bjc/azy052; Leitao, R. (2019), 'Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse', *DIS '19: Proceedings of the 2019 on Designing Interactive Systems Conference*, pp. 527–39, https://doi.org/10.1145/3322276.3322366; Slupska, J. and Tanczer, L. M. (2021), 'Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things', in Bailey, J., Flynn, A. and Henry, N. (eds), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, Leeds: Emerald Publishing Limited, pp. 663–88, https://doi.org/10.1108/978-1-83982-848-520211049; Levy, K. and Schneier, B. (2020), 'Privacy threats in intimate relationships', *Journal of Cybersecurity*, 6(1), https://doi.org/10.1093/cybsec/tyaa006.
40 See https://stopstalkerware.org.
41 Parkin, S., Patel, T., Lopez-Neira, I. and Tanczer, L. M. (2019), 'Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse', *Proceedings of the New Security Paradigms Workshop (NSPW '19)*, pp. 1–15, https://doi.org/10.1145/3368860.3368861.
42 Mehrnezhad, M. and Almeida, T. (2023), '"My sex-related data is more sensitive than my financial data and I want the same level of security and privacy": User Risk Perceptions and Protective Actions in Female-oriented Technologies', arXiv preprint arXiv:2306.05956, https://arxiv.org/abs/2306.05956; Almeida, T., Shipp, L., Mehrnezhad, M. and Toreini, E. (2022), 'Bodies Like Yours: Enquiring Data Privacy in FemTech', *Adjunct Proceedings of the 2022 Nordic Human-Computer Interaction Conference (NordiCHI '22)*, 54, pp. 1–5, https://doi.org/10.1145/3547522.3547674. For a study of health-related apps more broadly, see Grundy, Q. et al. (2019), 'Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis', *BMJ*, 364, l920, https://doi.org/10.1136/bmj.l920.
43 Pittman, A. (2022), 'The Internet Still Thinks I'm Pregnant', podcast, *New York Times*, 2 November 2022, https://www.nytimes.com/2022/11/02/podcasts/modern-love-internet-miscarriage.html.

apps are gendered by default, the harms that result are also inherently gendered. In this way, femtech privacy issues become part of a broader reduction and stigmatization of women's reproductive rights in many places worldwide.

Although conceptions of privacy are diverse and context-dependent, and change over time, gendered differences also appear in studies of attitudes to the misuse or exploitation of personal digital data. Oomen and Leenes concluded, in 2008, that 'gender appears not to influence privacy risk perception'.[44] In contrast, more than a decade later, Coopamootoo et al. identified a 'privacy gender gap' whereby 'women feel more negatively about [online] tracking, yet are less likely to take protective actions, compared to men'.[45] Such a perceived lack of security consciousness is, according to Wei et al., a prevalent gender stereotype.[46] Respondents to surveys conducted by those authors not only viewed women as more gullible, emotional and likely to share sensitive information on social media (thereby presenting a higher cybersecurity risk), but also viewed them as being less interested in and capable of adopting technical cybersecurity measures. Wei et al. trace such stereotypes to deeper forms of sexist essentialism, including the unfounded association of biological sex differences with ICT security behaviours.[47]

Such stereotypes inform the assessment made by Slupska et al. that cybersecurity concerns of women – and vulnerable gender identities in general – are more likely to be minimized or overlooked.[48] This is despite the fact that, in many cases, women face greater security burdens and are more likely to be affected by cybersecurity advertising that is misleading about the dangers they face.[49] More specifically, gendered victim-blaming often occurs in response to the sharing of explicit images, choosing weak passwords or clicking on phishing links.[50] The non-consensual dissemination of intimate images, in particular, is a growing form of gendered cyber harm, attracting attention in international cybercrime negotiations.[51]

---

44 Oomen, I. and Leenes, R. (2008), 'Privacy Risk Perceptions and Privacy Protection Strategies', in de Leeuw, E., Fischer-Hübner, S., Tseng, J. and Borking, J. (eds), *Policies and Research in Identity Management*, International Federation for Information Processing, 261, Boston, MA: Springer, https://doi.org/10.1007/978-0-387-77996-6_10.
45 Coopamootoo, K. P. L., Mehrnezhad, M. and Toreini, E. (2022), '"I feel invaded, annoyed, anxious and I may protect myself"': Individuals' Feelings about Online Tracking and their Protective Behaviour across Gender and Country', conference paper, 31st Usenix Security Symposium, https://www.usenix.org/conference/usenixsecurity22/presentation/coopamootoo. See also McGill, T. and Thompson, N. (2021), 'Exploring potential gender differences in information security and privacy', *Information and Computer Security*, 29(5), pp. 850–65, https://doi.org/10.1108/ICS-07-2020-0125; and Coopamootoo, K. P. L. and Ng, M. (2023), '"Un-Equal Online Safety?" A Gender Analysis of Security and Privacy Protection Advice and Behaviour Patterns', arXiv:2305.03680, https://doi.org/10.48550/arXiv.2305.03680.
46 Wei, M., Emami-Naeini, P., Roesner, F. and Kohno, T. (2023), 'Skilled or Gullible? Gender Stereotypes Related to Computer Security and Privacy', *IEEE Symposium on Security and Privacy*, pp. 2050–67, https://doi.ieeecomputersociety.org/10.1109/SP46215.2023.00023.
47 Ibid.
48 Slupska, J., Dawson Duckworth, S., Ma, L. and Neff, G. (2021) 'Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity', *CHI Conference on Human Factors in Computing Systems*, pp. 1–6, https://doi.org/10.1145/3411763.3451731.
49 Millar, Shires and Tropina (2021), *Gender approaches to cybersecurity*, p. 22.
50 Slupska, Dawson Duckworth, Ma and Neff (2021), 'Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity', p. 9.
51 Chatham House Cyber Policy team (2023), 'Submission to the 6th session of the Ad Hoc Committee (AHC) on cybercrime: gender considerations on the convention draft text', August 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/Chatham_House.pdf.

To summarize, a data breach is a cybersecurity issue because it is a privacy violation and involves (and can facilitate) unauthorized access to personal information that can then be 'weaponized' to cause harm online and offline. Data breaches through technology-facilitated abuse or femtech are gendered cybersecurity issues for two chief reasons. First, the impact of data breaches relies on gendered stereotypes of perceptions of, and attitudes towards, privacy and data protection. Second, the misuse of or access to digital data by those who do not have a right to access that data can be used to cause tangible harm and abuse to individuals, and there is a clear gendered element to this tactic.

3.3 State overreach

The third kind of gendered cyber harm stems from states' use of policy and legislation to advance and enforce certain state-aligned gender norms online. For example, cybercrime laws may include clauses criminalizing online content that contravenes public decency or morals, usually defined elsewhere in states' penal codes or criminal law, and often build on unequal standards of behaviour for people according to their gender. Similarly, cybersecurity strategies may leave the determination of what content constitutes a national security threat undefined, with state law enforcement or intelligence agencies then interpreting provisions through their own legal and institutional prisms. Where such agencies have histories of discrimination and repression against certain gender identities, sexualities or sexual orientations (online or offline), discriminatory practices are likely to manifest in law enforcement and other national practices in the digital space – often, but not always, in the name of cybersecurity and protecting against cybercrime.

While both hate speech and data breaches are cyber threats in a broadly conventional cybersecurity sense, where a malicious actor seeks to cause harm via technological means, the gendered harms resulting from state cybersecurity and cybercrime laws are less direct. In this case, the harm occurs not because of the cyber threat itself, but as part of a state response to counter cyber threats. This can be termed 'overreach', as the state response exceeds or omits what is strictly necessary to counter cyber threats while respecting gender and other human rights.

The imposition of rigid and exclusionary understandings of gender through cyber policy and legislation occurs as part of a broader phenomenon of cybersecurity measures facilitating authoritarian practices through control, surveillance and monitoring of digital public/private communication and content. There is an extensive body of research documenting the human rights implications of cybercrime laws, cybersecurity strategies and other similar measures that restrict fundamental freedoms (such as freedom of expression) online by authorizing

violations and imposing censorship.[52] In this way, the gendered harms that result from state cybersecurity measures are one – but far from the only – consequence of cybersecurity that is state-centric rather than human-centred.[53]

Such actions occur within broader state efforts to politicize and securitize gender, both online and offline. States have long created and supported narratives of gender that are closely intertwined with ideas of national identity and security. Such narratives are typically most explicit in wartime, although they persist outside of conflict. For example, states frequently mobilize concepts of hegemonic masculinity to aid military recruitment, as well as characterizing adversaries as a threat to an idealized femininity – national or otherwise.[54] Consequently, state law and regulation has historically enabled political bodies and systems to exert control over gender identities and expressions under the pretext of protecting against threats to national security (sometimes including, in a circular logic, the destabilization of prevalent gender norms itself as a national security threat).

There are three relevant implications of state overreach as regards cybersecurity and gender. First, understanding and acknowledgment of gendered cyber harms depends on the extent to which states leverage gender identities and gendered norms for purposes of national security and identity. Second, state responses to gendered cybersecurity vulnerabilities and risks will be prioritized or deprioritized in line with national gendered ideals and norms. Third, access to tools, systems and measures that mitigate such cybersecurity vulnerabilities and risks will depend on how a state (and other influential actors or communities in a given state context) supports or encourages specific understandings of gender. Overall, while the first two kinds of gendered cyber harm foreground the individual identity aspects of gender, state overreach foregrounds the role of gender as both social structure and system of power.

---

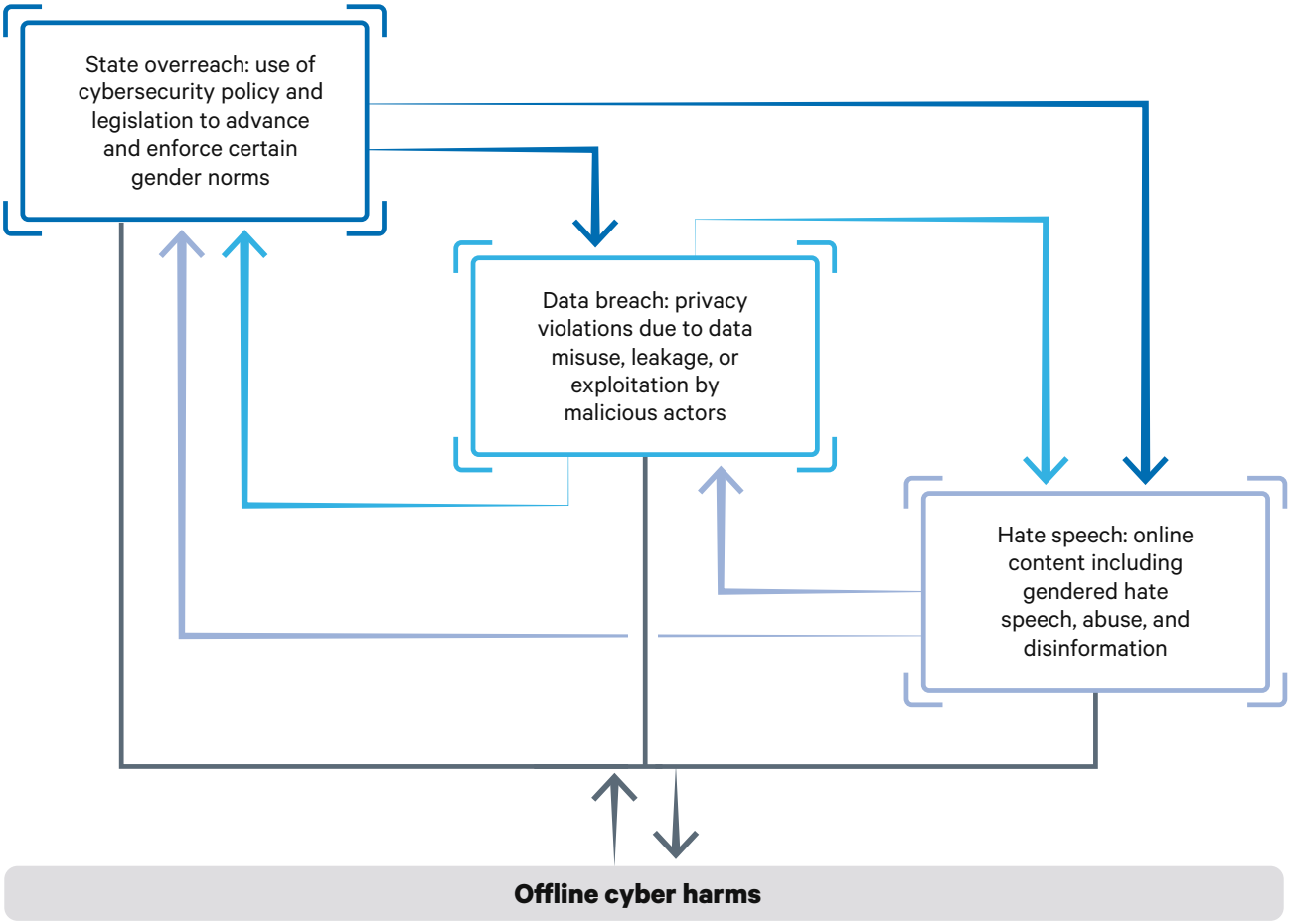
52 Hassib, B. and Shires, J. (2021), 'Manipulating uncertainty: cybersecurity politics in Egypt', *Journal of Cybersecurity*, 7(1), https://doi.org/10.1093/cybsec/tyaa026; Shires (2021), *The Politics of Cybersecurity in the Middle East*, London: Hurst Publishers.
53 Deibert, R. J. (2020), *Reset: Reclaiming the Internet for Civil Society*, Toronto: September Publishing.
54 Sjoberg, L. (2014), *Gender, War, and Conflict*, New York: Polity; Millar, K. M. (2022), *Support the Troops: Military Obligation, Gender, and the Making of Political Community*, Oxford: Oxford University Press.

04 Cascading and compounding gendered cyber harms

The three kinds of gendered cyber harms described in Chapter 3 are cascading and compounding. They are cascading because one form of gendered cyber harm leads to another; and they are compounding because such cascades increase the impact on those affected. Understanding gendered cyber harms as being cascading and compounding allows for a better understanding of how offline and online gendered harms interact and are mutually reinforcing (Figure 1).

This chapter analyses the cascading and compounding impacts of gendered cyber harms through an exploration of intersectional gender issues in selected political and social contexts. The first section, connecting online content and data privacy, examines misinformation and disinformation concerning abortion and reproductive health, along with potential privacy violations around femtech apps and devices. The second, connecting data privacy and state cybercrime laws, examines the cyber threats faced by LGBTIQ+ people using online dating apps, and LGBTIQ+ people's risk of exposure to state criminalization. The third, connecting online content and state cybercrime laws, examines abusive campaigns online against victims of sexual violence, and exacerbating or inadequate state responses. Each section focuses on the connection between two kinds of gendered harm, and also highlights where such connections go further to create a cascade of gendered harms between all three kinds.

Figure 1. Cascading and compounding gendered cyber harms



This analysis focuses on developments in six countries – the US, Poland, Indonesia, Uganda, Egypt and Brazil – drawing on secondary sources including academic articles, NGO reports and media coverage. The choice of countries is intended to show that cascading and compounding gendered cyber harms exist worldwide, across varying social and political contexts. With the caveat that global indexes provide limited comparative insight into the state of gender equality, online freedom and cybersecurity, a summary of relevant indexes for these six countries is provided in Table 1. These indexes provide global benchmarks for gender equality and cybersecurity for the six countries, but are not conclusive or definitive records or evidence of progress being made in either of those fields. Additionally, the indexes as portrayed here do not necessarily indicate a correlation between gender equality and cybersecurity.

Table 1. Gender, online freedom and cybersecurity indexes for selected countries

Country	OECD Social Institutions and Gender Index 2023[55] (score from very low to very high levels of institutional discrimination)	World Economic Forum Global Gender Gap Index[56] (score from 0–1; 1 equals parity)	PRIO/Georgetown Women, Peace, and Security Index 2023/2024[57] (score from 0–1; 1 is highest security)	Freedom House Freedom on the Net 2023[58] (ranking from 0–100; not free/ partly free/free	ITU Global Cybersecurity Index 2020[59] (score from 0–100; low to high)
US	Very low	0.748	0.823	76, free	100
Poland	Very low	0.722	0.859	Not included	93.86
Indonesia	Medium	0.697	0.700	47, partly free	94.88
Uganda	Low	0.706	0.544	51, partly free	69.98
Egypt	Very high	0.626	0.645	28, not free	95.48
Brazil	Low	0.726	0.630	64, partly free	96.6

Detailed social, political and legal context is vital to understanding the online and offline impacts of gendered cyber harms, including where offline gendered harms manifest online (i.e. when they are cyber-enabled), and where cybersecurity issues – broadly defined – are central to the presence of such harms (i.e. when they are cyber-dependent).

Gendered cyber harms do not, of course, occur only in the six countries discussed in this chapter; nor is the prevalence or severity of such harms exceptional in these countries. A more comprehensive global comparative analysis is beyond the scope of the paper, as similar harms may occur in nearly all countries and world regions. Even as regards these six countries, the paper does not make any claims regarding the frequency or severity of cascading or compounding gendered cyber harms. Instead, the examples cited are intended to be illustrative of the potential – in some cases, actual – links between different kind of gendered cyber harm.

55 Organisation for Economic Co-operation and Development (2023), *Social Institutions and Gender Index, SIGI 2023 Global Report: Gender Equality in Times of Crisis*, https://doi.org/10.1787/4607b7c7-en.
56 World Economic Forum (2023), *Global Gender Gap Report 2023*, Cologny/Geneva: World Economic Forum, https://www.weforum.org/publications/global-gender-gap-report-2023.
57 Georgetown Institute for Women, Peace and Security and Peace Research Institute Oslo (2023), *Women, Peace and Security Index 2023/24: Tracking sustainable peace through inclusion, justice, and security for women*, Washington, DC: GIWPS and PRIO, https://giwps.georgetown.edu/wp-content/uploads/2023/10/WPS-Index-executive-summary.pdf.
58 Shahbaz, A. et al. (eds) (2023), *Freedom on the Net 2023: The Repressive Power of Artificial Intelligence,* Washington, DC: Freedom House, https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-DigitalBooklet.pdf.
59 International Telecommunication Union (2021), *Global Cybersecurity Index 2020: Measuring commitment to cybersecurity*, Geneva: ITU, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

4.1 Connections between mis/disinformation and data privacy around abortion and reproductive health

Abortion rights and reproductive health are highly controversial political issues in many countries,[60] and recent legislative developments in the US and Poland demonstrate the fragility of access to safe and legal abortion for people who become pregnant. In the US, the Supreme Court's overturning of *Roe v. Wade* in June 2022 led to almost complete bans on abortion in 14 states in the following year.[61] The strictest of the revised state provisions, in Louisiana, does not allow exceptions in cases of rape or incest, although the actual implementation of similar exceptions in other states is far from clear.[62] Reflecting wider inequalities in the US healthcare system, one study estimated that in the hypothetical case of a total cessation of abortions across all US states, the number of maternal deaths would increase by 24 per cent; the greatest risk would be for non-Hispanic black people, with the estimated number of maternal deaths increasing by 39 per cent.[63]

In the case of Poland, the Constitutional Tribunal ruled in 2020 that access to abortion is unconstitutional in the case of severe and irreversible fetal abnormality or incurable illness that threatens the fetus's life. As a result, Polish law currently permits abortion only to safeguard the life or health of a woman, or where a pregnancy results from rape.[64] Even with such minimal exceptions, ambiguity around the law and grounds for prosecution – compounded by fears that a subsequent legal requirement for doctors to collect data on all pregnancies could in effect create a so-called 'pregnancy register'[65] – has caused some medical practitioners to refuse abortion procedures, leading to, in at least one case, the death of a pregnant woman.[66] Such steps form part of an incremental reduction in reproductive and gender rights in Poland since 2015, when the right-wing, conservative Christian and populist Law and Justice Party entered power.[67] Under the new administration formed by Donald Tusk following the 2023 legislative

---

60 Berer, M. (2017), 'Abortion Law and Policy Around the World: In Search of Decriminalization', *Health and Human Rights*, 19(1), pp. 13–27, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5473035.
61 Harte, J. (2023), 'Abortion rights supporters and opponents mark one year without Roe v. Wade', Reuters, 20 June 2023, https://www.reuters.com/world/us/abortion-rights-supporters-opponents-mark-one-year-without-roe-v-wade-2023-06-19.
62 Felix M., Sobel L. and Salganicoff, A. (2023), 'A Review of Exceptions in State Abortions Bans: Implications for the Provision of Abortion Services', KFF, https://www.kff.org/womens-health-policy/issue-brief/a-review-of-exceptions-in-state-abortions-bans-implications-for-the-provision-of-abortion-services.
63 Estimated percentage increases compared with 2020 levels of abortion access. Stevenson, A. J., Root, L. and Menken, J. (2022), 'The maternal mortality consequences of losing abortion access', *SocArXiv,* https://doi.org/10.31235/osf.io/7g29k.
64 Human Rights Watch (2020), 'Poland's Constitutional Tribunal Rolls Back Reproductive Rights', 22 October 2020, https://www.hrw.org/news/2020/10/22/polands-constitutional-tribunal-rolls-back-reproductive-rights.
65 Holt, E. (2022), 'Poland to introduce controversial pregnancy register', *The Lancet*, 399(10343), p. 2256, https://doi.org/10.1016/S0140-6736(22)01097-2.
66 Posner, L. (2022), 'Poland's New 'Pregnancy Registry' Raises Red Flags', Think Global Health, 17 June 2022, https://www.thinkglobalhealth.org/article/polands-new-pregnancy-registry-raises-red-flags.
67 Grant, R. (2023), 'The Conviction of Justyna Wydrzyńska', *The Nation,* 23 June 2023, https://www.thenation.com/article/society/justyna-wydrzynska-poland-abortion.

elections, there is the prospect of some liberalization of the country's abortion laws, but the broad political spectrum represented in his coalition government will influence how far-reaching – or restricted – any reforms may be.[68]

Abortion is the subject of much online misinformation (false information spread unintentionally) and disinformation (false information spread intentionally).[69] A study of Google searches in the US for 'abortion pill' found three of the top five results were anti-abortion websites peddling prevalent false claims about a pill's medical consequences and legal requirements.[70] A separate study by the same authors found most Google searches were conducted in US states with the strictest abortion laws.[71] Others have labelled abortion-related content as 'the next infodemic', borrowing the World Health Organization's term for the proliferation of false information about the COVID-19 pandemic.[72]

In 2022, research and analysis conducted by the Institute for Strategic Dialogue found that abortion content on major social media platforms was 'widespread and unchecked' and 'meant to instill uncertainty and fear'.[73] This included both high-profile pages and advertising content, the latter of which directly generates revenue for the platforms. The study also found global discrimination in platform policy and response measures, as information labels warning of potentially false or misleading content on YouTube videos did not appear unless accessed from some English-speaking countries.

Such content constitutes a gendered cyber harm, even without considering the online abuse and threats known to be experienced by pro-choice activists, advocates and politicians.[74] In political contexts where decisions on abortion have damaging consequences for people who are pregnant and people who conduct abortions, such misinformation and disinformation can either increase insecurity or perpetuate a false sense of security on an inherently gendered matter. The spread of this type of online content can be the result of lax privacy and security features and/or deliberate platform design choices, with the latter sometimes influencing the former,[75] and leads to insecurity offline as individuals

---

68 Easton, A. (2024), 'Polish MPs debate liberalising right to abortion on demand', BBC News, 11 April 2024, https://www.bbc.co.uk/news/world-europe-68786995; Amnesty International (2024), 'Poland: Vote is a significant step towards providing access to safe and legal abortion', 12 April 2024, https://www.amnesty.org/en/latest/news/2024/04/poland-vote-is-a-significant-step-towards-providing-access-to-safe-and-legal-abortion.
69 Barr-Walker, J. et al. (2021), 'Countering Misinformation About Abortion: The Role of Health Sciences Librarians', *American Journal of Public Health*, 111(10), pp. 1753–56, https://doi.org/10.2105/AJPH.2021.306471.
70 Pleasants, E., Guendelman, S., Weidert, K. and Prata, N. (2021), 'Quality of top webpages providing abortion pill information for Google searches in the USA: An evidence-based webpage quality assessment', *PLoS ONE*, 16(1), e0240664, https://doi.org/10.1371/journal.pone.0240664.
71 Guendelman, S., Pleasants, E., Cheshire, C. and Kong, A. (2022), 'Exploring Google Searches for Out-of-Clinic Medication Abortion in the United States During 2020: Infodemiology Approach Using Multiple Samples', *JMIR Infodemiology*, 2(1), e33184, https://infodemiology.jmir.org/2022/1/e33184.
72 Pagoto, S. L., Palmer, L. and Horwitz-Willis, N. (2023), 'The Next Infodemic: Abortion Misinformation', *Journal of medical Internet research*, 25, e42582, https://doi.org/10.2196/42582.
73 Martiny, C., Visser, F., and Jones, I. (2022), *Evaluating Platform Abortion-Related Speech Policies: Were Platforms Prepared for the Post-Dobbs Environment?*, Institute for Strategic Dialogue and CASM Technology, https://www.isdglobal.org/isd-publications/evaluating-platform-abortion-related-speech-policies-were-platforms-prepared-for-the-post-dobbs-environment.
74 Swash, R. and Strzyżyńska, W. (2022), 'Death threats and phone calls: the women answering cries for help one year on from Poland's abortion ban', *Guardian*, 23 January 2022, https://www.theguardian.com/global-development/2022/jan/23/death-threats-and-phone-calls-the-women-answering-cries-for-help-one-year-on-from-polands-abortion-ban.
75 Sharevski, F. et al. (2023), 'Abortion Misinformation on TikTok: Rampant Content, Lax Moderation, and Vivid User Experiences', arXiv:2301.05128, https://doi.org/10.48550/arXiv.2301.05128.

are denied important information and coerced into courses of action that might be life-threatening or a violation of their rights. Here, especially, we see how offline and online gendered harms can be mutually reinforcing.

Such gendered cyber harms, centered on the harmful consequences of online content, are compounded by the extensive collection of sensitive personal data by femtech devices and apps. Many femtech products collect directly or indirectly measured data on users' body temperature, sleep patterns and other pattern-of-life information, as well as data input by users on their menstrual cycle, for instance. In the past decade, the privacy and security practices of period-tracking and other femtech apps have come under scrutiny.[76] In one high-profile instance, the state of California concluded a settlement with a technology company investigated in connection with an app's 'serious privacy and basic security failures that put women's highly-sensitive personal and medical information at risk', including by allowing third parties access to a user's information without the user's consent.[77] A 2021 report by the International Digital Accountability Council found that some fitness and wellbeing apps – including period-tracking apps – sent unencrypted personal information to third parties, some of which were based in countries with 'weak data protection laws and a history of human rights abuses'.[78] The implications of poor data practices involving these types of mobile applications are global and extensive: combined with other socio-political gendered constructs, legislation and practices, the cascading and compounding harm is significant.

Data collection on an individual's menstrual cycle in general, and the lack of privacy protections around the sale, transfer and use of such data – as well as unclear requests for consent from the user – has generated new risks for pregnant people considering an abortion. In the US, the 2022 Supreme Court decision overturning *Roe v. Wade* was met with a flurry of concerns that data used to monitor and track periods and fertility could be 'weaponized' by health providers and used to prosecute people seeking abortions.[79] In Poland, the entry into force, in 2022, of the legal requirement for doctors to collect data on all pregnancies raised concerns over how such data could be used to intimidate or prosecute women and their families.[80]

---

76 Tiffany, K. (2018), 'Period-tracking apps are not for women', Vox, updated 16 November 2018, https://www.vox.com/the-goods/2018/11/13/18079458/menstrual-tracking-surveillance-glow-clue-apple-health.
77 State of California Department of Justice (2020), 'Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information', press release, 17 September 2020, https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-landmark-settlement-against-glow-inc-%E2%80%93; Beilinson, J. (2020), 'Glow Pregnancy App Exposed Women to Privacy Threats, Consumer Reports Finds', *Consumer Reports,* 17 September 2020, https://www.consumerreports.org/mobile-security-software/glow-pregnancy-app-exposed-women-to-privacy-threats-a1100919965. It is important to note that the company subsequently took remedial action and strengthened privacy features in subsequent app updates.
78 Williams, H., Kozemczak, G. and Kinney, D. (2021), *Digital Health is Public Health: Consumers' Privacy & Security in the Mobile Health App Ecosystem*, International Digital Accountability Council, https://0nh51b.p3cdn1.secureserver.net/wp-content/uploads/2022/01/Digital-Health-is-Public-Health-Consumers-Privacy-and-Security-in-the-Mobile-Health-App-Ecosystem.pdf.
79 Slupska, J. and Shipp, L. (2022), 'What you need to know about surveillance and reproductive rights in a post Roe v Wade world', The Conversation, 6 July 2022, https://theconversation.com/what-you-need-to-know-about-surveillance-and-reproductive-rights-in-a-post-roe-v-wade-world-185933.
80 Posner (2022), 'Poland's New 'Pregnancy Registry' Raises Red Flags'; Tayler, L. (2022), 'Two Years On, Poland's Abortion Crackdowns and the Rule of Law', Human Rights Watch, 22 October 2022, https://www.hrw.org/news/2022/10/22/two-years-polands-abortion-crackdowns-and-rule-law.

Some commentators consider that such fears could be overstated, arguing for instance that while 'data collected by fertility apps, tech companies and data brokers might be used to prove a violation of abortion restrictions, in practice, police and prosecutors have turned to more easily accessible data' such as online search histories.[81] While law enforcement agencies may continue to rely on the relatively high evidential standards of device browser records, a vast range of gendered cyber harms may result before any case reaches this stage. In particular, as social media platforms personally curate content, data flows between femtech apps and platform apps stored on the same device (and supposedly anonymized large-scale data resold via intermediaries) are more likely to result in tailored abortion misinformation and disinformation being delivered via an individual's personal feed.[82]

Other potential harms include technology-facilitated violence and abuse. It is possible, for instance, for an abusive partner to gain access to sensitive information related to an individual's reproductive health – a privacy violation in itself – and then use this information to control, manipulate or otherwise further harm that person. Examples of such harms include coercing a partner into unwanted pregnancy, denying them access to contraception, or using data or information from a device to instigate or underpin further offline harms.

While law enforcement agencies may continue to rely on the relatively high evidential standards of device browser records, a vast range of gendered cyber harms may result before any case reaches this stage.

Another area of potential harm relates to the availability and accessibility of femtech: denial-of-service attacks or other availability threats to femtech providers could, for instance, limit users' access to important time-sensitive information. This area of risk demonstrates the importance of a broad and human-centred understanding of what constitutes 'critical infrastructure', entailing going beyond information and digital infrastructures of national or economic significance to also include those infrastructures that underpin social lives and individual experiences.[83]

It is important to understand that violations in femtech data privacy can be directly connected to false and misleading online content about abortion and reproductive health. These two forms of gendered cyber harm cascade both ways. On the one hand, femtech data could contribute to social media algorithms determining what ads, pages or content an app user is shown, including about abortion; and, on the other hand, proliferation of harmful online content around policy and regulatory shifts could create a 'legitimizing' environment for data breaches and privacy

81 Zakrzewski C., Verma P. and Parker C. (2022), 'Texts, web searches about abortion have been used to prosecute women', *Washington Post*, 3 July 2022, https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution.
82 Conti-Cook, C. (2020), 'Surveilling the Digital Abortion Diary', *University of Baltimore Law Review*, 50(1), https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2.
83 Bernarding and Kobel (2023), *Feminist Perspectives on the Militarisation of Cyberspace*.

violations. The issues also compound, as together they increase the overall level of harm to individuals and groups affected. The compounding harm is most starkly experienced by women being denied vital healthcare and/or being exposed to abuse and discrimination.

Here, a range of technical, social and individual factors together create an environment of digital and physical insecurity. This insecure environment cannot be corrected only through better data protection and better cyber hygiene regarding the use of technologies to enable or facilitate personal decisions. Both are required, but they need to be accompanied by stronger state protection for vulnerable or at-risk individuals, together with meaningful efforts to understand and respond to gendered security issues – be these in healthcare or in cyberspace.

4.2 Cybersecurity risks to LGBTIQ+ communities

The rights of LGBTIQ+ people are curtailed across the world. Since 2015, the LGBTIQ+ community in Indonesia – a majority Muslim country with a largely secular constitution – has faced 'creeping criminalization', including campaigns to ban discussion of LGBTIQ+ rights on university campuses, an Islamic legal opinion calling for corporal punishment of same-sex relations, and increasingly inflammatory rhetoric from regional and national politicians.[84] A former defence minister, while in office, described homosexuality as 'a kind of modern warfare' that was undermining the country's sovereignty.[85] The country's long-anticipated new criminal code, approved by parliament in December 2022, effectively criminalizes consensual sex outside of marriage. Marriage between same-sex couples is not permitted in Indonesia, and Human Rights Watch warned that, although the crimes of extramarital sex or cohabitation can only be prosecuted if the complainant is the spouse, parent or child of the accused, women and LGBTIQ+ people would be disproportionately affected by the new provisions since they are more likely to be reported for infidelity or for relationships those family members disapprove of.[86]

---

84 Wieringa, S. E. (2019), 'Criminalisation of Homosexuality in Indonesia: The Role of the Constitution and Civil Society', *Australian Journal of Asian Law*, 20(1), pp. 227–45, https://ssrn.com/abstract=3488561; Nadia, M. (2017), *Shifting Boundaries and Contentions: The Regulation of "Victimless Crimes" in Indonesia*, Arryman Fellow Research Paper, Northwestern University, Illinois, https://www.edgs.northwestern.edu/documents/051217.mirna.arryman-paper.pdf.
85 Kapoor, K. and Da Costa, A. B. (2018), 'Criminal code revamp plan sends chill through Indonesia's LGBT community', Reuters, 9 February 2018, https://www.reuters.com/article/us-indonesia-lgbt-insight-idUSKBN1FT2IO; BBC News (2016), 'The sudden intensity of Indonesia's anti-gay onslaught', 29 February 2016, https://www.bbc.co.uk/news/world-asia-35657114.
86 Human Rights Watch (2022), 'Indonesia: New Criminal Code Disastrous for Rights', 8 December 2022, https://www.hrw.org/news/2022/12/08/indonesia-new-criminal-code-disastrous-rights.

In Uganda, a majority Christian country, a growing conservative movement has been financially and politically supported by some US Christian evangelical fundamentalist groups for at least 20 years.[87] These groups have campaigned against gender equality and LGBTIQ+ rights in Uganda through preaching, political connections and the media.[88] Homosexuality has long been indirectly criminalized through the British colonial-origin penal code, although a 2014 Anti-Homosexuality Act, which made provision for punishment of 'aggravated homosexuality' with life imprisonment, was swiftly annulled (ostensibly on procedural grounds) following opposition from human rights defenders within Uganda and international (especially US government and UN) pressure.[89] A new Anti-Homosexuality Act was signed into law in 2023.[90]

In both Indonesia and Uganda, there is a clear slide towards online abuse, discrimination and vilification of LGBITQ+ identities and communities – i.e. hate speech, as described in Chapter 3. There is also state overreach on the part of each country, as legislation criminalizes LGBTIQ+ activities. Uganda's 2023 legislation includes the use of 'a computer, information system or the internet' in its criminalization of 'promotion of homosexuality', explicitly adding a cyber element to the criminalization of LGBTIQ+ activities.[91] In Indonesia in 2018, two men operating a Facebook account to arrange meetings for gay people were charged under the 2008 electronic information law for 'creating and transmitting pornographic content'.[92] The Indonesian government also sought to progressively impose various kinds of censorship on social media platforms for the same

---

87 Kaoma, K. (2009), 'The U.S. Christian Right and the Attack on Gays in Africa', Political Research Associates, 1 December 2009, https://politicalresearch.org/2009/12/01/us-christian-right-and-attack-gays-africa. See also the Uganda case study in McAlister, M. (2023), 'Evangelicals and Human Rights', in Sabatini, C. (ed.) (2023), *Reclaiming Human Rights in a Changing World Order*, Washington, DC and London: Brookings Institution Press and Royal Institute of International Affairs, pp. 165–69, https://www.chathamhouse.org/2022/10/reclaiming-human-rights-changing-world-order/7-evangelicals-and-human-rights; Burnham, J. (2022), 'Fighting Familiar Wars on Foreign Shores: Disinformation, the American Right, and Uganda', NATO Association of Canada, 12 August 2022, https://natoassociation.ca/fighting-familiar-wars-on-foreign-shores-disinformation-the-american-right-and-uganda.

88 Namubiru, L. and Wepukhulu, K. S. (2020), 'U.S. Christian Right pours more than $50m into Africa', openDemocracy, 29 October 2020, https://www.opendemocracy.net/en/5050/africa-us-christian-right-50m.

89 UN News (2014), 'Annulment of Uganda's anti-homosexuality law hailed by UN officials', 1 August 2014, https://news.un.org/en/story/2014/08/474242. For additional context, see Sexual Minorities Uganda (2014), *Expanded Criminalisation of Homosexuality in Uganda: A Flawed Narrative*, Kampala: Sexual Minorities Uganda (SMUG), https://www.humandignitytrust.org/wp-content/uploads/resources/Expanded-Criminalisation-of-Homosexuality-in-Uganda-2014.pdf.

90 Budoo-Scholtz, A. (2023), 'Uganda's President Signs Repressive Anti-LGBT Law', Human Rights Watch, 30 May 2022, https://www.hrw.org/news/2023/05/30/ugandas-president-signs-repressive-anti-lgbt-law; Peel, D. (2023), 'The politics behind Uganda's Anti-Homosexuality Act', Death Penalty Research Unit Blog, https://blogs.law.ox.ac.uk/death-penalty-research-unit-blog/blog-post/2023/12/politics-behind-ugandas-anti-homosexuality-act.

91 Amnesty International (2023), 'Uganda: President's approval of anti-LGBTI Bill is a grave assault on human rights', https://www.amnesty.org/en/latest/news/2023/05/presidents-musevenis-approval-of-anti-lgbti-bill-is-a-assault-on-human-rights; Office of the Clerk to Parliament (2023), 'Motion Seeking Leave of Parliament to Introduce a Private Members' Bill entitled "Anti-Homosexuality Bill"', 28 February 2023, https://uploads.guim.co.uk/2023/03/01/Motion_Seeking_Leave_of_Parliament_to_Introduce_a_Private_member%27s_Bill_Entitled_%27Anti-Homosexuality_Bill%27_(1).pdf; The Republic of Uganda (2023), 'The Anti-Homosexuality Act, 2023', https://www.parliament.go.ug/sites/default/files/The%20Anti-Homosexuality%20Act%2C%202023.pdf.

92 Reuters (2018), 'Indonesian police arrest two men linked to LGBT Facebook page', 21 October 2018, Reuters, https://www.reuters.com/article/uk-indonesia-lgbt-idUKKCN1MV08O.

reason, including via efforts to ban same-sex emojis in 2016,[93] and requesting that Google remove 73 LGBTIQ+ apps – including the gay dating app Blued – from its Google Play Store in 2018.[94]

Online abuse and criminalization under information and cybercrime laws are not the only cybersecurity risks to which LGBTIQ+ people in Uganda and Indonesia are exposed. Some reports suggest that advanced spyware and surveillance software has been used to target LGBTIQ+ communities, constituting a privacy violation in addition to hate speech and state overreach. In Uganda in 2014, shortly after the country's then anti-homosexuality legislation was enacted, the civil society organization Unwanted Witness warned that LGBTIQ+ people were being targeted by phishing attacks that installed what was, at that time, thought to be a form of the well-known 'Zeus' cybercriminal malware.[95] Subsequently, in 2015 Buzzfeed News conducted an analysis of emails leaked by Wikileaks that, they argued, showed that the (now defunct) Italy-based spyware company Hacking Team had discussed selling its software to the Ugandan government. In one internal email, an engineer had observed that cybersecurity firms 'think we are a new Zeus'.[96] Hypothetically, the gendered cyber harms from malicious software in general (including data leaks, blackmail and ransom) can be compounded by the potential for such software to aid digital and physical repression by the state, through collecting intelligence identifying individuals for arrest or intimidation, and providing evidence for conviction under the legislation discussed above.

Similarly, according to a *Haaretz* investigation in 2018, the Indonesian government purchased surveillance software to 'create a database of LGBT rights activists who had been targeted for surveillance'.[97] In 2019, one Grindr user in Indonesia observed that the app had become 'full of escorts, drug dealers, and undercover police', and that 'extortion [by police] is common'.[98] The normative and practical links between institutionalized discrimination by the state and the broader phenomenon of 'sextortion' by primarily non-state criminal actors apparently underscore that not only does sextortion rely on a sense of shame amplified by threat of legal sanction, but in some states members of law enforcement agencies themselves may be perpetrators of blackmail and extortion.

Overall, gendered cyber harms in Uganda and Indonesia are cascading: online abuse appears to be used by law enforcement agencies to identify people who are LGBTIQ+, who are then subject to state surveillance and criminal prosecution

---

93 Associated Press via *Guardian* (2016), 'Indonesia bans gay emoji and stickers from messaging apps', 12 February 2016, https://www.theguardian.com/world/2016/feb/12/indonesia-bans-gay-emoji-and-stickers-from-messaging-apps.
94 Gay Star News via Medium (2018), 'Google blocks gay dating app Blued after requests from Indonesian government', 1 February 2018, https://medium.com/gsn-gay-star-news/google-blocks-gay-dating-app-blued-after-requests-from-indonesian-government-8d227f6e7e5d.
95 Unwanted Witness (2014), 'LGBTI online community experiencing "Zeus malware"', 24 April 2014, https://www.unwantedwitness.org/unwanted-witness-uw-news-brief-lgbti-online-community-experiencing-zeus-malware.
96 Frenkel, S. (2015), 'These Two Companies Are Helping Governments Spy On Their Citizens', Buzzfeed News, 24 August 2015, https://www.buzzfeednews.com/article/sheerafrenkel/meet-the-companies-whose-business-is-letting-governments-spy.
97 Shezaf, H. and Jacobson, J. (2018), 'Israel's Cyber Spy Industry Helps World Dictators Hunt Dissidents and Gays', *Haaretz*, 20 October 2018, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000.
98 Faber, T. (2019), 'Grindr around the world', *The Face,* 29 November 2019, https://theface.com/society/grindr-illegal-lgbt-dating-egypt-indonesia-iran-jamaica-uganda.

via data misuse and privacy violations. These gendered cyber harms are also compounding, in that LGBTIQ+ people, and especially activists within LGBTIQ+ communities, must consider all these risks simultaneously in seeking to fully express their sexual orientation and gender identity. The cybersecurity measures necessary to enable this full expression are broad and holistic, spanning better cyber hygiene, strong data protection, and processes, strategies and legislation to counter and reduce online abuse and hate speech.

An increase in repression, first targeting LGBTIQ+ communities and then moving towards broader gendered discrimination and the criminalization of a wider range of 'sexual offences' to underpin conservative gender norms, suggests that, in some contexts, cyber threats to LGBTIQ+ communities might be an early indicator of a wider shift in negative government policies and attitudes to diverse gender expression in general – and gendered cyber harms in particular. In the context of a deepening suppression, seen in many countries worldwide, of diverse aspects of gender identity, a focus on a particular community, group or individual provides an entry point for later and wider expansion of gender-insensitive policies.

4.3 Misogynistic hate speech and discriminatory cybercrime prosecutions

In many jurisdictions, cybercrime laws exist to curb and prosecute cybercriminal activity. However, there is little consensus at global level on what constitutes a 'cybercrime' and what is within the scope of cybercrime legislation. This ambiguity – together with the extension of the offline world to the online world and the sheer scope of potential criminality online – has enabled some countries to include so-called 'morality clauses' in cybercrime laws. These clauses or provisions in cybercrime laws – i.e. legislation that is intended as a cybersecurity measure – have been used to oppress and criminalize dissidents, activists and human rights defenders in multiple countries. While ostensibly in place to prevent or deter cybercrime, morality clauses in cybercrime laws often embody conventional and traditional gendered norms and stereotypes, and are used to enforce gendered behaviour online and criminalize behaviour that does not conform with offline social standards or norms.[99] Additionally, they are often ambiguously defined and arbitrarily applied. This has cascading and compounding consequences: the inclusion of morality clauses in cybercrime laws creates an enabling environment to enforce gendered norms online, leading to the over-criminalization of women and LGBTIQ+ communities and facilitating misogynistic hate speech towards those who are perceived to be non-conforming in online spaces.

In Egypt, a majority Muslim country with a substantial Coptic Christian minority, the main legislative tool for state enforcement of prevalent gender norms until early 2020 was the 1961 Law on Combating Prostitution, especially Article 9(c), concerning 'whoever habitually engages in debauchery or prostitution', and Article 14(a), criminalizing incitement to or publicity of debauchery. In more

99 Human Rights Watch (2021), 'Abuse of Cybercrime Measures Taints UN Talks', Human Rights Watch, 5 May 2021, https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks.

recent years, digital evidence from dating apps, chats and photos or videos found on individuals' devices was frequently used as evidence in the prosecution of people accused of engaging in acts of consensual gay sex, along with prosecutions of transgender people and other gender-nonconforming identities and practices.[100] However, challenges from defence lawyers and NGOs successfully focused on the 1961 law's requirement for an element of publicity (i.e. committing an act publicly), which was difficult to prove based solely on private conversations on users' devices.

Instead, prosecutors began to try 'morality' cases in the economic courts, created in 2008, which have jurisdiction over the 2003 Telecommunication Regulation Law and the 2018 Anti-Cyber and Information Technology Crimes Law, in addition to other financial and economic laws. Article 76 of the Telecommunication Regulation Law criminalizes the 'misuse of telecommunications'; and Article 25 of the Anti-Cyber and Information Technology Crimes Law criminalizes the use of technology to 'infringe on any family principles or values in Egyptian society', with a minimum sentence of six months.

In recent years in Egypt, digital evidence from dating apps, chats and photos or videos found on individuals' devices was frequently used as evidence in the prosecution of people accused of engaging in acts of consensual gay sex, along with prosecutions of transgender people and other gender-nonconforming identities and practices.

In July 2020, five women social media influencers (the youngest of whom was 17 years old), were convicted by the economic court under Egypt's Anti-Cyber and Information Technology Crimes Law, in connection with content that they had posted on TikTok. Two of the women were each given two-year prison sentences and fined $18,000.[101] On appeal, one of the two was acquitted and the other had her sentence overturned; however, the same women were subsequently convicted on criminal charges of 'human trafficking', ultimately receiving six- and three-year sentences.[102] Such use of cybercrime and telecommunications laws in the courts system in effect functions to police women's public representation of their bodies and identities.

In contrast, cybercrime law enforcement action appears to overlook serious crimes of sexual violence that include cyber elements. In some jurisdictions – including Egypt – the combination of state overreach in some cases and lax enforcement in others risks exacerbating the discriminatory effects of morality-based

---

100 Egyptian Initiative for Personal Rights (2017), *The Trap: Punishing sexual difference in Egypt*, Cairo: Egyptian Initiative for Personal Rights, https://eipr.org/en/publications/trap-punishing-sexual-difference-egypt.
101 Nabil, S. (2020), 'Egypt TikTok and Instagram stars pay heavy price for 'indecency', BBC News, 17 August 2020, https://www.bbc.co.uk/news/world-middle-east-53733841.
102 BBC News (2022), 'Egypt female TikTok star jailed for three years for human trafficking', 18 April 2022, https://www.bbc.co.uk/news/world-middle-east-61139566.

cybercrime legislation and can potentially act as an enabler for misogynistic hate speech around such incidents, retraumatizing and compounding the harms inflicted on victims.

For example, in one such case, a woman posted a video via TikTok in which she recounted having been raped. The post went viral, and images of her assault were subsequently released online. The victim was herself then detained under morality-related charges.[103] She was released shortly afterwards, and five of the people she accused were sentenced over the next two years.[104] The combination of lax (and subjective) enforcement of cybercrime laws and state overreach had clear cascading and compounding effects: the women was a victim of rape, and the perpetrators posted images of her assault online without her consent (a clear privacy violation). These images – and the woman's viral video – led to victimization and misogyny on social media, and an improper application of legislation that resulted in the woman's detention. It is important to note that the cascading and compounding impacts of such cases are ongoing: the repercussions facilitate the further cascading and compounding of gendered cyber harms, hindering women's participation in online spaces, with negative effects on social equality, political participation and democracy.

These negative consequences for social equality, political participation and democracy are not endemic to one country or one region. Women politicians all over the world are openly and frequently subjected to online misogyny and sexist and gendered abuse. Concerning Brazil, for example, studies of online abuse against candidates during municipal elections in 2020 highlighted the intersectional nature of such abuse: Black women were victims of racial and gendered discrimination, and transgender councillors also suffered increased abuse.[105] One study emphasizes how such abuse is enmeshed with prevalent concepts of masculinity.[106] Another connects it to a broader 'masculine crisis' of economic origins.[107] Most starkly, the murder, in 2018, of a Black, bisexual city councillor, Marielle Franco, highlighted the connection between online misogyny in politics and physical violence. Supporters of Jair Bolsonaro – a candidate for the presidency at the time of Franco's death – launched disinformation campaigns designed to undermine Franco's legacy and deter the (online and offline) feminist

---

103 Human Rights Watch (2020), 'Egypt: Spate of 'Morality' Prosecutions of Women: Arrests, Jail for Violating 'Family Values'', 17 August 2020, https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women.
104 *Ahram Online* (2021), 'Court sentences five people to prison for kidnapping, rape of underage Tiktoker', 24 May 2021, https://english.ahram.org.eg/NewsContent/1/64/412785/Egypt/Politics-/Court-sentences-five-people-to-prison-for-kidnappi.aspx.
105 Azmina Magazine and Internet Lab (2021), *MonitorA: Report on online political violence on the pages and profiles of candidates in the 2020 municipal elections*, São Paulo: Revista AzMina and InternetLab, https://www.internetlab.org.br/wp-content/uploads/2021/03/5P_Relatorio_MonitorA-ENG.pdf; Davidziuk, M. I. and Davidziuk, M. A. (2009), *Mexico, Argentina, Brazil and Colombia: Cross-country Study on Violence against Women and Information Communication Technologies*, GenderIT.org, https://genderit.org/resources/mexico-argentina-brazil-and-colombia-cross-country-study-violence-against-women-and; de Pinho, T. R. (2023), 'Violence against Women in Politics in Brazil: An Instrument of Power and Anti-Egalitarian Oppression', Social Science Research Council Items, 28 February 2023, https://items.ssrc.org/democracy-papers/democratic-anxieties-in-the-americas/violence-against-women-in-politics-in-brazil-an-instrument-of-power-and-anti-egalitarian-obstruction.
106 Azmina Magazine and Internet Lab (2021), *MonitorA: Report on online political violence on the pages and profiles of candidates in the 2020 municipal elections*.
107 D'Ávila, M. (2022), 'Violence in social media threatens women active in Brazilian politics', Heinrich Böll Stiftung, 27 September 2022, https://www.boell.de/en/2022/09/13/violence-social-media-threatens-women-active-brazilian-politics.

mobilization that followed her death.[108] At the same time, it has been argued that Franco's murder was a catalyst for a 'transformation of feminist debates on online gender-based violence in Brazil'.[109]

Similar risks extend to people working in the media sector, too: a 2021 study by Reporters Without Borders demonstrated how journalists in Brazil also face overlapping threats from gender-based and political disinformation and abuse on social media, further underscoring that online violence generates offline violence.[110]

Recent legislation in Brazil has sought to address online misogyny, including on social media platforms. These efforts exemplify an important aspect of the relationship between state legislation and online abuse from a gendered perspective: while state overreach in itself can be a source of gendered harm, legislative changes can also be crucial in tackling gendered cyber harms. Three important new laws were enacted in 2021. The first two criminalized, respectively, stalking online and offline (Law 14.132) and the infliction of psychological violence on women (Law 14.188).[111] The third law, passed in August 2021 (having been repeatedly tabled and redrafted since 2014), sought specifically to prevent and combat violence against women in politics, as well as criminalizing election disinformation (Law 14.192).[112] These new measures built on a longer history of increased legal protections for women in situations of gender-based violence, especially an eponymous law introduced in 2006 after campaigning by Maria da Penha, a Brazilian human rights defender and activist.[113] Other Brazilian legislation also enables victims of non-consensual intimate images dissemination (NCIID) to file civil lawsuits or private criminal prosecution.[114] Such legislative developments point to and encourage a broadening conception of cybersecurity that elevates online disinformation and abuse as a security priority[115] and emphasizes the fluidity between offline and online gendered harms. While

---

108 Di Meco, L. and Wilfore, K., (2021), 'Gendered disinformation is a national security problem', Brookings Institute, https://www.brookings.edu/articles/gendered-disinformation-is-a-national-security-problem.
109 Sívori, H. and Mochel, L. (2022), *Brazilian feminist responses to online hate speech: Seeing online violence through an intersectional lens,* Latin America Center on Sexuality and Human Rights (CLAM), https://www.apc.org/en/pubs/brazilian-feminist-responses-online-hate-speech-seeing-online-violence-through-intersectional.
110 Reporters without Borders (2022), 'Brazil: Disinformation and online attacks against women journalists pose serious challenges to the exercise of press freedom in the country', 26 April 2022, https://rsf.org/en/news/brazil-disinformation-and-online-attacks-against-women-journalists-pose-serious-challenges-exercise.
111 Mascotte, L. and Santos, L. M. (2021), 'Legal Developments to Combat Violence Against Women in Brazil', Oxford Human Rights Hub, 20 September 2021, https://ohrh.law.ox.ac.uk/legal-developments-to-combat-violence-against-women-in-brazil.
112 James, E. (2021), 'Gender-Based Violence Legislation Passed in Brazil After Six Years', International Republican Institute, 30 November 2021, https://www.iri.org/news/gender-based-violence-legislation-passed-in-brazil-after-six-years; Library of Congress (2021), 'Brazil: New Law Enacted to Combat Political Violence Against Women', 13 August 2021, https://www.loc.gov/item/global-legal-monitor/2021-08-13/brazil-new-law-enacted-to-combat-political-violence-against-women.
113 Griffin, J. (2016), 'The woman behind Brazil's domestic violence law: 'I can't give up the fight'', Reuters, 2 September 2016, https://www.reuters.com/article/us-brazil-women-abuse-idUSKCN1181PJ.
114 Valente, M. (2018), 'Do we need new laws to address non-consensual circulation of intimate images: the case of Brazil', GenderIT.org, 17 June 2018, https://genderit.org/articles/do-we-need-new-laws-address-non-consensual-circulation-intimate-images-case-brazil; Rocha, R. de L. M., Pedrinha, R. D. and Oliveira, M. H. B. de (2019), 'O tratamento da pornografia de vingança pelo ordenamento jurídico brasileiro' [The treatment of revenge pornography by the Brazilian legal system], *Saúde em Debate*, 43(4), pp. 178–89, https://doi.org/10.1590/0103-11042019S415; Neris, N., Ruiz, J. P. and Valente, M. G. (2018), *Fighting the Dissemination of Non-Consensual Intimate Images: a comparative analysis*, InternetLab, http://www.internetlab.org.br/wp-content/uploads/2018/11/Fighting_the_Dissemination_of_Non.pdf.
115 Devanny, J. and Buchan, R. (2023), *Brazil's Cyber Strategy Under Lula: Not a Priority, but Progress Is Possible*, Washington, DC, Carnegie Endowment for International Peace, 8 August 2023, https://carnegieendowment.org/2023/08/08/brazil-s-cyber-strategy-under-lula-not-priority-but-progress-is-possible-pub-90339.

not all are explicitly cybersecurity measures, they demonstrate growing awareness of the need to safeguard women's participation in online spaces and shore up their security in cyberspace.

Despite this substantial shift in relevant legislation in Brazil, new legal protections remain insufficient due to their limited implementation and tendency to be subsumed by wider gendered assumptions and cultures in politics and law enforcement. A 2020 study, for instance, found that court judgments on online gender-based violence did not use the term 'hate speech' or consider women as a group targeted by such abuse.[116] According to one academic, there is an 'active, almost militant form of sexism entrenched in the entire [Brazilian] legal system', making success very difficult for lawsuits regarding online gender-based violence, and domestic violence courts more generally.[117] Some progress has been made: notably, for instance, victims of NCIID can request urgent protective measures, with such claims processed through specialist domestic violence courts.[118] However, resort to prosecution is highly dependent on financial and educational status, leading to class-based inequalities in access to justice.[119] This lack of recognition that such violence is gender-*based*, or that gender should be considered a protected category or characteristic, highlights how entrenched attitudes and norms impede prosecution of online misogyny, leading to its continuation – and thus further gendered cyber harms – even when the legislative tools to combat it exist.

Overall, in both Egypt and Brazil, the gendered cyber harms resulting from online misogyny and sexism in the criminal justice system are closely related. These harms cascade in both directions: as the targeting of politicians along with gender and women's rights activists in Brazil shows, seeking to achieve justice for instances of online gender-based violence generates further violence online, while online abuse itself leads to – and is met with – gendered assumptions and judgments in the courts. They also compound, as the same victims suffer the consequences of both kinds of harm. However, the cases of Egypt and Brazil are different in important respects: Egypt's cybercrime law itself contains discriminatory elements, exacerbated further by law enforcement agencies' interpretation and practice; in Brazil, there has been a significant move towards greater legal protections against gendered cyber harms. Consequently, and unlike Egypt, Brazil is not a case of legislative 'state overreach' causing gendered cyber harms. Instead, there are tensions between different parts of the state – in particular between relevant new legislation and the judiciary – which result in discriminatory cybercrime prosecutions and, in consequence, cybersecurity that is not gender-sensitive or gender-transformative.

---

116 Martins, F. K. et al. (2020), 'Violence against women online and the courts: preliminary observations', *InternetLab,* 12 November 2020, https://internetlab.org.br/en/news/violence-against-women-online-and-the-courts-preliminary-observations.
117 Bird, H. (2020), 'Victims of Domestic Violence and Restorative Justice: Some Notes from the 'Periphery' to the 'World Centres'', Oxford Centre for Criminology All Souls Blog, 6 November 2020, https://blogs.law.ox.ac.uk/centres-institutes/centre-criminology/blog/2020/11/all-souls-blog-victims-domestic-violence-and.
118 Council of Europe (2022), *The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform*, Thematic paper of the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW), Brussels, https://www.ohchr.org/sites/default/files/documents/hrbodies/cedaw/statements/2022-12-02/EDVAW-Platform-thematic-paper-on-the-digital-dimension-of-VAW_English.pdf.
119 Valente (2018), 'Do we need new laws to address non-consensual circulation of intimate images: the case of Brazil'.

In both cases, connecting risk areas and better understanding their intersection can help reduce gendered cyber harms that result from a combination of state legislation, cyber insecurity, and social stigma and discrimination. The isolation of policy areas (including, but not limited to, content moderation and mis/disinformation), legislative tools to combat privacy violations and discrimination, and the social and legal manifestation of gendered norms together contribute to the overall risk landscape. Feminist methodologies and principles and gender analyses of proposed measures and mechanisms to tackle security issues can help ensure all legislation and national strategies are designed and implemented in a gender-sensitive way, to advance rather than impede gender equality.

05 Conclusion and recommendations

This paper has argued that gendered cyber harms are cascading and compounding: hate speech and data breaches can each inflict further harm on people who are already victims of the other, and both can be exacerbated by state overreach, inattention and discrimination. This insight enhances the existing literature on gender and cybersecurity by highlighting the need to connect different areas of research and advocacy in order to better understand and combat gendered cyber harms in a holistic way. By identifying the connections between gendered cyber harms, state policy and practice can better counter and mitigate those harms.

The paper has demonstrated the cascading and compounding nature of gendered cyber harms through illustrative examples from a selected group of countries. The analysis highlights how gendered cyber harms cascade between misinformation and disinformation and data misuse due to failings to ensure robust privacy protections for sensitive personal data. It shows how LGBTIQ+ communities are particularly exposed to cascading and compounding gendered cyber harms from hate speech, data breaches and state overreach, highlighting the vulnerability of personal devices to malicious spyware and the physical and digital insecurities of online dating apps. And it argues that gendered cyber harms can occur because of – or, in the case of Brazil, despite – state legislation designed to improve or enhance cybersecurity and gender equality.

Overall, the discussion demonstrates four key points:

1. The scope of cybersecurity is larger than just the technical security of computer systems; it encompasses the experiences of everyone who uses computer systems, and the perceptions of safety and security that users attach to these technologies and systems. Such experiences and perceptions are impossible to dissociate from an individual's identity, and ultimately impact how digital technologies affect their life and contribute to their security. The case studies in this paper have shown how experiences and perceptions of security and insecurity in cyberspace can be shaped by factors beyond purely technical ones.

2. The relationship between gendered harms offline and gendered harms in cyberspace is mutually reinforcing. Offline harms give rise to online harms, which in turn have offline and online consequences. All the case studies discussed in this paper have demonstrated cascading harms, whereby harms in one area give rise to other harms.
3. Cybersecurity is inherently gendered because it is derived from and built on a set of political, social and security beliefs and assumptions that are gendered. If national and international security does not consider gender security to be a security matter, cybersecurity will continue to exacerbate gendered harms. This is demonstrated by, for instance, the use of 'morality clauses' in some countries' cybercrime laws.
4. Gendered cyber harms – and, by extension, the gendering of cybersecurity – are a global problem that manifests differently depending on social, political and security contexts.

This study, which itself draws on extensive work by others, points to the need for still further research. The analysis in Chapter 4 focuses on illustrative examples of the connections between different kinds of gendered cyber harms in six countries, selected to demonstrate that cascading and compounding gendered cyber harms exist worldwide, across varying social and political contexts. While this approach is sufficient for demonstrating the global nature of cascading and compounding gendered harms, and the need for international attention and cooperation, further in-depth research into connected gendered cyber harms in specific country contexts is required.

Furthermore, the paper – and the policy recommendations that follow – focus on the actions of and security conditions created and nurtured by states. With hate speech, data breaches and state overreach, technology design, ownership and operation occur largely in multinational companies, and these organizations are crucial stakeholders in a rapidly evolving landscape. While this paper does not consider their role further, a second paper in this series will focus specifically on technology companies and their role in furthering a gender-responsive and gender-transformative approach to cybersecurity.

Policy recommendations

The case studies in this paper underscore the important role that state actors need to play in encouraging an empowering and gender-sensitive cyber landscape, and fostering a robust and gender-transformative interpretation and vision of cybersecurity. Globally, more states are developing an awareness of, or acknowledging, gender dimensions in cybersecurity. This is demonstrated in national strategies, international initiatives and multilateral forums. However, more work needs to be done to tackle gendered cyber insecurity, ranging from updating legislation to working with international partners on building capacity to better understand and combat gendered cyber harms. This paper concludes by addressing the question of what states – irrespective of national gender norms –

can and should do to address the gendered harms that emanate from cybersecurity risks and vulnerabilities, and sets out general recommendations for how the different kinds of gendered harms can be connected and addressed holistically.

Recommendation 1: Combine technical, social and individual factors when analysing cyber threat and risk

Gendered cyber harms are technological, social and psychological. As such, states' analyses of cyber threats and risks should take into account their impact on technologies, people and communities, incorporating considerations based on gender and other intersectional identities. Risk analysis should incorporate a full understanding of the cascading and compounding nature of gendered cyber harms as a key component of risk management and mitigation. Vulnerability analysis should avoid victim-blaming or attributing cyber incidents excessively to the 'human factor'. For example, while phishing links are a common vector for malicious software, and users often agree to vastly complex social media terms and conditions without reading them, these are symptoms of systemic problems, rather than failures on the part of individuals. Because gendered cyber harms arise from a combination of technical, social and individual factors, an equally holistic approach is necessary to counter them. From a state perspective, this combination of analyses might entail cross-governmental initiatives and research, or diversifying the expertise and analyses of those responsible for devising and implementing policy solutions.

Recommendation 2: Ensure that the security of at-risk, marginalized and minoritized groups is treated as seriously as that of other national security assets and interests

Explicitly, this entails improving data protection, privacy rights and cyber hygiene for everyone. The speed of technological development and the adversarial nature of many cyber threats means that specific countermeasures are likely to become outdated quickly. It also means that new targets and victims become vulnerable in new and more ways. States should seek to implement and encourage broad privacy protections for personal data, along with easy-to-implement cyber hygiene measures, with additional protections for at-risk groups such as minoritized or disproportionately targeted communities, politicians, journalists, human rights defenders and activists. To take cybersecurity risks to LGBTIQ+ communities as an example, improved cyber hygiene for LGBTIQ+ people to help them safely navigate cyberspace (e.g. through education on what information (not) to share online, how to use location services, etc.) is, in isolation, insufficient to increase their cybersecurity substantially; it also places the responsibility for security or safety on the victim, often without proportionate efforts to discourage and deter perpetrators. While this is not a gender-specific recommendation, it advances gender equality indirectly by ensuring that protecting at-risk groups is a priority on par with protecting national assets and infrastructure (or traditional security priorities). Unless online abuse and hate speech are addressed as – and elevated to – a cybersecurity concern, improving cyber hygiene alone will not reduce gendered insecurity or gendered cyber harms.

Recommendation 3: Adopt a gender-sensitive and human-centred approach to cybersecurity and cybercrime

Appropriate cybersecurity and cybercrime strategy, policy and implementation is crucial to ensuring victims of gendered cyber harms can access justice and receive appropriate care. This paper has shown that state anti-cybercrime actions can – at times unintentionally – exacerbate or introduce new gendered harms. States should draw on resources such as the Association for Progressive Communications' (APC) assessment tool for assessing the gender impact of national cybersecurity strategies,[120] together with Chatham House's Strategic Approach to Countering Cybercrime (SACC) framework and its associated *Integrating gender in cybercrime capacity-building* toolkit.[121] These approaches include the adoption of feminist methodologies and principles in designing cybersecurity protections. Feminist methodologies and principles acknowledge and seek to counteract structural inequalities (economic, class and others) and power imbalances between gendered and other groups. Using such approaches in cybersecurity necessitates centrally incorporating the perspectives of victims of cyber threats, as well as people and/or groups who might use technologies in unexpected or undesigned ways, and addressing wider dependencies between different technologies and social relationships.

Recommendation 4: Increase knowledge and coordination across different agencies and organizations working on cyber

States should work both domestically and internationally to institutionalize coordination between organizations, departments, agencies and teams working on technical cybersecurity, cybersecurity legislation, gender policy and measures to counter disinformation. This can help states identify where gendered cyber harms extend across these different specialist areas, and to avoid contradictions in state policy and practice. For example, setting up regular exchanges and mechanisms for information-sharing between teams working in or on each of these areas can improve awareness of interconnected gendered harms and the cybersecurity risks and vulnerabilities that lead to and exacerbate these harms, both offline and online. Across the illustrative examples of gendered cyber harms in this paper, better coordination across the monitoring and countering of online abuse and hate speech, data protection and legislative tools could have led to a better understanding of the threat landscape for vulnerable people and groups, leading to more effective protections.

120 Association for Progressive Communications (2022), 'A framework for developing gender-responsive cybersecurity policy', https://www.apc.org/en/pubs/framework-gender-cybersec.
121 Emerson-Keeler, Swali and Naylor (2023), *Integrating gender in cybercrime capacity-building: a toolkit*.

Final remarks

In sum, cybersecurity is better, more inclusive, more resilient and more effective when it actively and deliberately considers the threats and risks that people might face, because of their gender, when they interact with cyberspace and digital technologies. Gendered cyber harms are a core cybersecurity problem: digital platforms, devices and technologies all have characteristics and functionalities that can amplify gendered harms, and gendered harms are exacerbated by cybersecurity measures and tools that fail to consider a gendered threat landscape. The existence of these harms contributes to national and international insecurity, inhibiting the development of a secure, safe, responsible and peaceful cyberspace for everyone. Understanding gendered cyber harms as cascading and compounding shows how offline and online gendered harms interact, intersect and reinforce one another to create a cyberspace that is inequitably insecure. Broadening states', institutions' and individuals' understanding of what constitutes cybersecurity, and how insecurity in cyberspace manifests, and is experienced and perceived, can lead to better policy responses and a more secure digital future.

About the authors

Dr James Shires is a former senior research fellow in Chatham House's International Security Programme. He is currently the co-director of the European Cyber Conflict Research Initiative (ECCRI) and the European Cyber Conflict Research Incubator (ECCRI CIC). James speaks, writes and teaches on a range of topics concerning politics, security and technology, especially cybersecurity (cyber threats to individuals, organizations and states, capacity-building, resilience and expertise) and information flows (disinformation, leaks and new media). He is the co-author of *Gender approaches to cybersecurity: design, defence and response* (UNIDIR, 2021) and *Gender Equality, Cybersecurity, and Security Sector Governance* (DCAF, 2022).

Dr Bassant Hassib is a non-resident scholar with the Strategic Technologies and Cybersecurity Program at the Middle East Institute. She was previously an assistant professor of political science at the British University in Egypt, a fellow at the Leicester Institute for Advanced Studies (LIAS) at the University of Leicester, and a DAAD visiting researcher at Arnold Bergstraesser Institute of the University of Freiburg. Dr Hassib's research areas and expertise include cybersecurity governance in Egypt and the GCC, (counter)surveillance, gendered cybersecurity threats, the geopolitics of cybersecurity and the digital economy, counterterrorism and civil society, military cyber and AI capabilities, the securitization of cryptocurrencies in MENA, and knowledge production in social sciences.

Amrit Swali is a research associate in Chatham House's International Security Programme and part of the editorial team of the institute's Journal of Cyber Policy. Amrit is also the co-chair for gender on Chatham House's Equality, Diversity and Inclusion Working Group. Amrit's research work focuses on cybercrime policies, international cyber governance and the intersection between gender, international security and cyber. She is co-author, with Rebecca Emerson-Keeler and Esther Naylor, of *Integrating gender in cybercrime capacity-building: a toolkit* (Chatham House, 2023).

Amrit holds an MSc in the history of international relations from the London School of Economics and Political Science, and a BA in history from the University of Southampton.

Acknowledgments

We are grateful for the support of the UK's Integrated Security Fund for enabling this project, and to the Foreign, Commonwealth and Development Office's (FCDO) Gender, Peace and Security team in the Office for Conflict, Stabilisation and Mediation project for their guidance and support in its delivery. This paper, the first of two in a series on gender and cybersecurity, advances understanding of how gendered cyber harms shape experiences and perceptions of cybersecurity in general, and how policy responses could mitigate these harms. The second paper in this series will focus specifically on technology companies and their role in furthering a gender-responsive and gender-transformative approach to cybersecurity.

We thank the project's advisory group and the International Security Programme at Chatham House for their feedback on early versions of this paper, particularly Joyce Hakmeh and Isabella Wilkinson. We also thank Jo Maher in the Communications and Publishing Department at Chatham House, and are grateful to the anonymous peer reviewers, members of FCDO and of the Global Cyber Alliance for their feedback.

Cover image: A protester takes a selfie in Warsaw, Poland, on 26 October 2020, during a demonstration against a constitutional tribunal ruling resulting in a near-total ban of abortion.
Photo credit: Copyright © Jaap Arriens/NurPhoto/Getty Images

ISBN 978 1 78413 597 3
DOI 10.55317/9781784135973

Cite this paper: Shires, J., Hassib, B. and Swali, A. (2024), *Gendered hate speech, data breach and state overreach: Identifying the connections between gendered cyber harms to shape better policy responses*, Research Paper, London: Royal Institute of International Affairs, https://doi.org/10.55317/9781784135973.

This publication is printed on FSC-certified paper.
designbysoapbox.com

Independent thinking since 1920

UK International Development

Partnership | Progress | Prosperity

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700
contact@chathamhouse.org | chathamhouse.org

Charity Registration Number: 208223