DCAF Geneva Centre for Security Sector Governance

Gender Equality, Cybersecurity, and Security Sector Governance

UNDERSTANDING THE ROLE OF GENDER IN CYBERSECURITY GOVERNANCE

Katharine Millar, James Shires, Tatiana Tropina

About DCAF

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice and supports capacity-building of both state and non-state security sector stakeholders.

ISBN 978-92-9222-674-9

Cover Photo credit: shutterstock_2136788105

This publication was developed within the framework of 'Good Governance in Cybersecurity in the Western Balkans', a DCAF – Geneva Centre for Security Sector Governance project, generously supported by the United Kingdom's Foreign, Commonwealth and Development Office.

THIS PAPER CONSIDERS THE FOLLOWING QUESTIONS:

- What is the relationship between gender and cybersecurity?
- How does gender equality help to achieve good cybersecurity governance?
- What are the main cybersecurity-specific challenges to incorporating gender equality into security sector governance?

INTRODUCTION

Cybersecurity – the broad array of security challenges presented to states, corporations, communities, civil society, and individuals arising from the use of information and communications technologies (ICTs) – is increasingly recognized as an important component of national and international security.[1] As with all aspects of security governance, the good governance of cybersecurity is defined by, and depends upon, gender equality. This paper maps the relationship between gender equality and cybersecurity governance as a component of good security sector governance (SSG). It outlines the applicability of existing tools and principles of good governance to cybersecurity, especially those concerning gender equality. It also discusses distinct challenges in cybersecurity that may require new strategies of governance – or the creative application of existing ones. Here, it highlights the way in which cybersecurity spans not only the conventional security sector (military, policing, justice, immigration, and so on) but also other areas of society, such as the private sector, which are not always considered relevant to national and international security.

1. What are gender and gender equality?

Gender refers to the socially and culturally constructed roles, expectations, attributes, and values within a given society associated with masculinity and femininity at a given time. Though gender is often understood as expressing expectations about appropriate behaviour for men and women, it is non-binary and diverse. Gender also, importantly, refers to the arrangement of social relations, distribution of resources, and access to power and opportunities between men, women, and people of non-binary and diverse gender identities and expressions.[2]

Gender is also increasingly understood as being intersectional: existing alongside multiple forms of social power

Gender is also increasingly understood as being **intersectional**: existing alongside multiple forms of social power relating to class, race, coloniality, nationality, ability, ethnicity, caste, sexual orientation,

1. Key international efforts to develop frameworks, norms, and laws for governing cyberspace include the UN Open-Ended Working Group on ICTs in the Context of International Security (OEWG, 2019 to present), the UN Global Group of Experts on Advancing Responsible Behaviour in Cyberspace in the Context of International Security (GGE, 2006-2021), and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC, 2022 to present). These efforts are accompanied by regional frameworks and initiatives, such as the Council of Europe's Budapest Convention on Cybercrime, the African Union's Convention on Cyber Security and Personal Data Protection, and the NATO-supported but non-binding Tallinn Manual on the International Law Applicable to Cyber Warfare.

2. UN Women Training Centre eLearning Campus, Gender Equality Glossary (New York: UN Women). https://trainingcentre.unwomen.org/mod/glossary/view.php?id=36&mode=letter&hook=G&sortkey=&sortorder=asc

age, and more.[3] This means that gender equality requires thinking about all experiences, capacities, and vulnerabilities of women, men, and people of diverse gender identities and expressions, to avoid inadvertently perpetuating less visible but related forms of inequality. For instance, though gender is distinct from **sexual orientation** – a person's emotional and/or romantic attraction to other people[4] – heterosexual attraction to people of the opposite sex is often a societal gender expectation of men and women. As a result, bisexual, lesbian, and gay people of all gender identities may experience stigma, discrimination, and violence. It is therefore important to consider sexuality when working for gender equality, as well as the range of other social factors described above.

Gender equality means 'equal rights, opportunities, and outcomes for girls and boys and men and women' and people of diverse gender identities and expressions.[5] Gender equality is a human right stated in the Charter of the United Nations and confirmed in many other international commitments.[6] The promotion of gender equality includes policy that addresses gender-based violence (GBV), an umbrella term for any harmful act – physical, emotional, sexual, psychological – that is perpetrated against a person's will and is based on socially ascribed (gender) differences attributed to men and women, stemming from a binary understanding of gender.[7]

2. What is the relationship between gender and security?

Gender relates to security in two ways.[8] First, men, women, girls, boys, and people of diverse gender identities and expressions have different security vulnerabilities, capacities, and needs. For instance, although people of all gender identities experience insecurity in conflict, men, boys, and people who read as male/masculine may be specifically targeted and killed in war (or forcibly conscripted) due to the gendered assumption that all men and boys are combatants, or potential combatants.[9] Likewise, while it is true that women, girls, and people who read as female/feminine experience GBV in conflict – including but not limited to sexual violence – women are subject to stereotypes that assume that they are always/only victims in war. This inattention to women's roles as combatants, peace activists, politicians, civil society actors, and so on can lead to women's exclusion from peace negotiations, conflict prevention, policymaking, and reconstruction policy programmes.[10]

3. Crenshaw, Kimberle, 'Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Colour', Stanford Law Review, vol. 43, no. 6, July 1991, pp. 1241–1299. https://doi.org/10.2307/1229039; and Combahee River Collective, 'A Black Feminist Statement', Women's Studies Quarterly, vol. 42, no. 3/4, Fall/Winter 2014, pp. 271–280. https://www.jstor.org/stable/24365010

4. United Nations Free and Equal, *Definitions*. https://www.unfe.org/definitions/

5. United Nations Office on Drugs and Crime, *Gender Mainstreaming in the Work of UNODC: Guidance Note for UNODC Staff* (Vienna: UNODC, 2021). https://www.unodc.org/documents/Gender/20-04944_Gender_Note_final_ebook_cb.pdf

6. These commitments include the Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW, 1979), the Beijing Declaration and Platform for Action (1995), and the Security Council Resolution 1325 on Women, Peace, and Security (2000).

7. Myrttinen, Henri, *Gender and Security Toolkit 1: Security Sector Governance, Security Sector Reform, and Gender*, p.7. Geneva Centre for Security Sector Governance (DCAF), OSCE/ODIHR, and UN Women, 2019. https://www.dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-1%20EN%20FINAL_2.pdf. See also UN Women, Gender Equality Glossary. https://trainingcentre.unwomen.org/mod/glossary/view.php?id=36; UN High Commissioner for Human Rights, *Discriminatory laws and practices and acts of violence against individuals based on their sexual orientation and gender identity*, UN Doc. A/HRC/19/41, 17 November 2011, para. 20.

8. See DCAF, OSCE/ODIHR, and UN Women, *Gender and Security Sector Reform Toolkit* (Geneva: DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit

9. Carpenter, R. Charli. 'Recognizing gender-based violence against civilian men and boys in conflict situations, in *The Criminology of War*, pp. 377-397 (Routledge, 2017).

10. Office of the United Nations High Commissioner for Human Rights (OHCHR), *Women's human rights and gender-related concerns in situations of conflict and instability.* https://www.ohchr.org/en/women/womens-human-rights-and-gender-related-concerns-situations-conflict-and-instability

> Gendered beliefs and assumptions about security influence what is seen as a security threat, how security threats are prioritized, and security resource allocation

Second, gendered beliefs and assumptions about security influence what is seen as a security threat, how security threats are prioritized, and security resource allocation. For instance, because state and military security organizations are often largely staffed by men, and associated with masculine attributes such as power, authority, and public protection, the security of the state is often prioritized over that of individuals (particularly women, people of diverse gender identities and expressions, and marginalized peoples) and civil society organizations (CSOs). Conventional national security threats, such as war and terrorism, are also often prioritized over threats that mainly produce insecurity for individuals and communities (such as poverty, displacement, environmental degradation, and GBV).

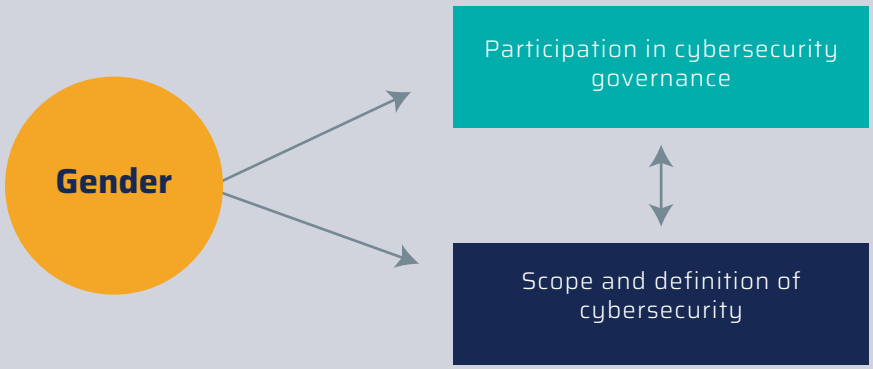
In short, people of all gender identities and expressions have the right to security. Gender equality in security governance therefore means looking both at how men, women, and people of diverse gender identities and expressions experience security challenges differently and how gendered norms and assumptions affect how we think about and prioritize different forms of insecurity. Gender equality in security governance also means ensuring that men, women, and people of diverse gender identities and expressions have equal opportunities to participate in security governance.

3. What is the relationship between gender and cybersecurity?

These same factors – gendered experiences of insecurity, gendered assumptions about security, and gender parity in participation in security governance – are all relevant to cybersecurity. They are complicated, however, by a lack of agreement regarding the meaning of cybersecurity. Although cybersecurity, broadly, refers to threats involving the use of ICTs, the central presence of ICTs in virtually every aspect of daily life for billions of people around the world means that almost all security issues have a 'cyber' component. It is therefore important to pay attention to how gendered assumptions and values can inform the definition of cybersecurity – with implications for the security experiences of men, women, and people of diverse gender identities and expressions. Decisions about what is and what is not a cybersecurity issue reflect and reinforce pre-existing patterns of (intersectional) gender inequality, including GBV, and have the potential to create new ones.

This relationship is illustrated in Figure 1. Gender directly affects the scope and definition of cybersecurity governance, because security issues – including cybersecurity ones – fundamentally incorporate gendered assumptions and expectations, as already discussed. Gender also directly affects participation in cybersecurity governance, as there are significant levels of gender (and other intersectional) inequalities in the skills and attributes perceived as necessary for cybersecurity governance – as detailed in the following paragraphs. Finally, gender indirectly but mutually affects both scope and participation via the other, so gender inequalities in participation further reinforce gendered understandings of the scope of cybersecurity, and gendered perceptions of a 'narrow' definition of cybersecurity attract and filter participants along similarly gendered lines. The remainder of this section explores this triple relationship in more detail, using illustrative examples where appropriate.

Figure 1: Gender impacts on cybersecurity governance



Gender and cybersecurity participation

Women, people of diverse gender identities and expressions, and men all have the right and should have the capacity to seek, receive, and impart information using the Internet,[11] participate in public affairs through online tools,[12] access cybersecurity/ICT education, work in technical ICT/cyber professions, and participate in cybersecurity governance and oversight. At present, however, women (and, likely, people of diverse gender identities and expressions, though data on this are sparse) are under-represented in nearly all aspects of cybersecurity participation.

Women's Internet access globally, for instance, is estimated to be at 85 per cent that of men; and approximately 1.7 billion women in the Global South lack Internet access. This disparity is a serious human rights concern that underlies all dimensions of cybersecurity, from potential exposure to insecurity to participation in governance. It is known as the **gender digital divide**.[13]

The science, technology, engineering, and mathematics (STEM) professions that are (typically) the precursor to technical cybersecurity roles are (with national variations) characterized by a gender gap between men and women (sometimes known as the '**digital skills gap**').[14] This gap has complex, context-specific causes that include a) inequities in access to infrastructure (the gendered digital divide) and education; b) individual and family-level constraints and priorities; and c) the continuation of sociocultural and institutional gender norms that suggest that STEM professions (and technical skills/capacities) are predominantly masculine/for men.[15] This gendered disparity in STEM education and training – sometimes referred to as the '**pipeline problem**'[16] – contributes to, but does not solely cause, gender disparities in participation in technical cybersecurity professions.

11. UN Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/HRC/17/27, Para. 20-21 (UN General Assembly, 2011). https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf

12. Ibid., Para. 62. See also: OHCHR, *Report of the Office of the United Nations High Commissioner for Human Rights: Good practices and challenges faced by States in using the guidelines on the effective implementation of the right to participate in public affairs*, A/HRC/49/42, Para. 10. https://www.ohchr.org/en/calls-for-input/2021/report-good-practices-and-challenges-using-guidelines-participation

13. Wajcman, Judy, Erin Young, and Anna Fitzmaurice, The Digital Revolution: Implications for gender equality and women's rights 25 years after Beijing (UN Women, 2020). https://www.unwomen.org/en/digital-library/publications/2020/08/discussion-paper-the-digital-revolution-implications-for-gender-equality-and-womens-rights; and Devillard, Sandrine, Anu Madgavkar, and Janet Bush, *A Woman's Place Is in the Digital Revolution* (Project Syndicate, 2018). https://www.project-syndicate.org/commentary/women-in-the-digital-revolution-by-sandrine-devillard-and-anu-madgavkar-2018-08?barrier=accesspaylog

14. Millar, Katharine, James Shires, and Tatiana Tropina, *Gender approaches to cybersecurity: design, defence and response* (UNIDIR, 2021), footnote 86. https://unidir.org/publication/gender-approaches-cybersecurity. See also Wajcman, Young, and Fitzmaurice (2020), op. cit.

15. Ibid., p. 33, footnote 87.

16. Vitores, A. and A. Gil-Juárez, 'The trouble with "women in computing": a critical examination of the deployment of research on the gender gap in computer science', *Journal of Gender Studies* (2006), *25*(6), pp. 666-680.

It is estimated that only approximately 24 per cent of cybersecurity professionals globally are women.[17] This is despite the fact that early computer science and coding were relatively open to women.[18] Computing came to be socially and culturally constructed as masculine/for men only as it grew in importance to the formal economy (and in social prominence and prestige).[19] Women also have a higher attrition rate in technology posts than men; a 2016 study in the US found that women were twice as likely to leave technology-based roles.[20] A 2017 study of women in cybersecurity found that 87 per cent reported experiences of implicit discrimination and 19 per cent experienced overt, explicit discrimination.[21]

The importance of **gender parity** in cybersecurity governance and negotiations has been recognized at the international level. The final report of the UN Open-ended Working Group on ICTs in the Context of International Security (OEWG), for instance, affirmed the importance of women's participation in international cybersecurity decision-making and encouraged states to take action, and build capacity, to empower women to do so.[22] State delegations to the UN Ad Hoc Committee on Cybercrime (AHC) have also highlighted the importance of gender equality in addressing and governing cybercrime and cyber law enforcement. States have begun to recognize the importance of linking cybersecurity with the Women, Peace and Security (WPS) Agenda,[23] which establishes women's participation in security governance as a key component of gender equality and human rights. Within these international processes, however, as well as in most national jurisdictions, there is still a long way to go before gender parity is reached in cybersecurity governance, implementation, and oversight.

Overall, though women are key cybersecurity actors, from technical experts to policymakers, gender parity in all aspects of cybersecurity remains an important goal that is yet to be achieved. Better data are also required to understand the experience and support the participation of people of diverse gender identities, expressions, and sexual orientations within the cybersecurity sphere. A key – though not deterministic – component of promoting gender parity within cybersecurity is to address: a) gendered biases and assumptions that suggest that STEM and computing are masculine/for men and; b) a related gendered hierarchy that privileges this more technical STEM and computing expertise associated with masculinities over other important cybersecurity capacities and fields, such as policymaking, governance, ethics, and oversight.

17. Millar, Shires, and Tropina (2021) op. cit., p. 31 footnote 80.

18. See for instance, Stross, Randall, 'What Has Driven Women Out of Computer Science?', *New York Times* (16 November 2008). http://classtap.pbworks.com/f/Women%20Driven%20From%20Computer%20Science%20Field.pdf

19. Light, J.S., 'When computers were women', *Technology and Culture*, 40(3) (1999), pp. 455-483.

20. Wacjman, Young, and Fitzmaurice (2020), op. cit., p. 12.

21. Millar, Shires, and Tropina (2021), op. cit., p. 31 footnote 81.

22. See Sharland, Lisa et al. *System Update: Towards a Women, Peace and Cybersecurity Agenda* (UNIDIR, 2021), pp 11-15. https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

23. UN General Assembly, A/AC.290/2021/CRP.3, para. 37. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf. For more on cybersecurity and the UN WPS Agenda, see Sharland et al. (2021), op. cit., pp. 15-19.

Gendered understandings of the scope of cybersecurity and its threats

Cybersecurity is often understood in terms of state security, related to the integrity of digital networks and systems key to **national defence** (including 'critical infrastructure'), and the use of hacking tools for state intelligence and military cyber operations (known as 'offensive cyber capabilities').[24] As with conventional security, this definition prioritizes public activities often associated with men and masculinity. Another central aspect of conventional understandings of cybersecurity is **private or corporate**, seeking to preserve the confidentiality, integrity, and availability (the 'CIA triad') of organizations' networks, systems, and/or information.

The harms to which individuals – particularly women; girls; people of diverse gender identities, expressions, and sexual orientations; marginalized and minoritized communities; and as part of civil society – are often exposed are not included in this definition, nor is their right to security. Women and girls may be particularly targeted by hacking of personal email and/or social media accounts, the use of keylogging software, and the use of 'spyware' as a continuation of family/intimate partner violence and stalking. While people of all genders are vulnerable to the leaking of private medical information via hacking, there are gendered risks of discrimination, stigmatization, and violence to people who may become pregnant, if their reproductive history or related information is revealed by a data breach.[25] Similarly, people of diverse gender identities, expressions, and sexual orientations are at risk of being targeted as a result of medical (and other) breaches of data privacy.[26] Distributed denial-of-service (DDOS) attacks – cyber attacks intended to shut down specific ICT systems, networks, or devices by flooding them with mundane communication requests – can also exacerbate gender inequality. For instance, though further research on gender and DDOS attacks is required, initial evidence suggests that such attacks may exacerbate pre-existing patterns of gender inequality by, for instance, bringing down the mobile e-commerce sites and micro-banking and financial transfer systems that many women small traders rely upon, pushing them into financial precarity.[27]

The limited, state- or corporation-centric definition of cybersecurity thus appears to be **gender-neutral** – assuming that the threats it addresses affect people of all genders in the same way. In making this assumption, however, the definition of cybersecurity is **gender-blind** – ignoring the ways in which cyber threats affect women, men, and people of diverse gender identities and expressions differently. A gender perspective suggests that we should move from state- or corporate-centric concepts to individual or human-centric approaches, seeing harms to individuals (as well as marginalized and minoritized communities) as issues of cybersecurity as much as questions of national security or corporate economic loss.

24. For the importance of gender equality, and a gender lens in understanding national intelligence practice and governance, see Hutton, Lauren, *DCAF Gender and Security Tool 14: Gender and Intelligence* (DCAF, 2019). https://www.dcaf.ch/sites/default/files/publications/documents/GSToolkit_Tool-14%20EN%20FINAL_0.pdf

25. For an overview, see Slupska, Julia and Laura Shipp, '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. For examples of incidents that pose such risks, see: Privacy International, 'Why Does Reproductive Health Surveillance in India Need Our Urgent Attention? (24 February 2020). https://privacyinternational.org/long-read/3368/why- does-reproductive-health-surveillance-india-need-our-urgent-attention; Davis, Jessica, '300,000 Records Breached in Ransomware Attack on Pennsylvania Health System', *Healthcare IT News* (26 July 2017). https://www.healthcareitnews.com/news/300000-records-breached-ransomware-attack-pennsylvania-health-system; and Hernandes, R., 'Gestão Haddad expõe na internet dados de pacientes da rede pública', *Folha de S.Paulo* (6 July 2016). https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da- rede-publica.shtml

26. For examples of cybersecurity failures that posed such risks, see BBC News, 'Trans Charity Mermaids UK "Deeply Sorry" for Data Breach' (16 June 2019). https://www.bbc.co.uk/news/uk-48652970; and Fox, Chris, 'Gender identity clinic leaks patient email addresses', BBC News, (6 September 2019). https://www.bbc.co.uk/news/technology-49611948

27. Brown, Deborah and Allison Pytlak, *Why Gender Matters in International Cyber Security* (Women's International League for Peace and Freedom and the Association for Progressive Communications, 2020), pp. 10-11. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. The gendering of DDOS attacks may also work in the other direction: for example, by prioritizing relatively temporary or trivial incidents targeted at 'core' state national security or financial institutions. A similar logic may also be observed with 'defacement' incidents; see, for example, Ben-David, Ricky, 'Israel's cyber directorate issues annual warning ahead of Iran's "Jerusalem Day"', *The Times of Israel* (22 April 2022). https://www.timesofisrael.com/israel-cyber-directorate-issues-annual-warning-ahead-of-irans-jerusalem-day/

Cybersecurity can also be defined in terms of the way that a harmful action relates to the use of ICTs, rather than the threatened actor (for example, the state vs the individual). Cybersecurity may be understood narrowly as preventing **malicious interference** with computer systems and devices (for example, hacking, denial-of-service, phishing, and so on), as well as the unauthorized interception (and/or alteration) of information (for instance, data breaches, identity theft). This is the definition most commonly used by technical cybersecurity practitioners.[28]

However, this definition risks being gender-blind in assuming that cyber operations affect people of all genders similarly – or, indeed, that it is only systems, not people, that are vulnerable to malicious interference.[29] It also does not capture gendered harms due to the manipulation, exploitation, or deliberate withdrawal of or lack of access to digital technologies.

Instead, cybersecurity could be defined more broadly to refer to protection against **individual, community, and societal harms related to the use of ICTs**. This might include concerns regarding artificial intelligence, the design of technology, and algorithmic and data bias. Such a broad understanding of cybersecurity could potentially also include issues of online content and social media, such as disinformation, deepfakes, hate speech, and harassment. Although broadening the concept brings problems of coherence and useability, the key point is that the scope of cybersecurity should be defined by the people who suffer most from ICT-related harms.

This broader definition of cybersecurity captures more gendered experiences. Most starkly, Internet shutdowns – even if directed by a government, rather than occurring due to a cyber operation – can expose women, girls, and people of diverse gender identities and expressions to physical insecurity by depriving them of the use of mobile phones and/or requiring them to navigate public places in the dark.[30] In another example, most big data sets – increasingly used, via algorithms, to draw inferences about the social world and inform government policy – either aggregate results drawn from studies of men or assumptions about a universalized 'reference' man and extrapolate them to people in general.[31] Artificial voice assistants, conversely, are frequently given feminine voices and names as default settings, reinforcing inequitable gender norms.[32] Facial recognition software has well-established gendered and racial biases.[33] The same is frequently true for the design of technology interfaces and products. For instance, smart home technologies frequently assume the home to be an equitable and safe place to be secured against outsiders; the 'threat modelling' of the design does not take into account the potential for safe home technology to be used as a means of surveillance, coercive control, and domestic abuse.[34]

28. Most cybersecurity analyses would differentiate between these examples in much finer detail: for example, between vectors of access (for instance, phishing), whether persistent access is required (it usually is for data breaches, but not for DDOS), and the 'actions on objectives' after access is achieved (leaks, identify theft, exfiltration, and so on).

29. See Millar, Shires, and Tropina (2021), op. cit. A focus on technological systems rather than people or social relations is arguably also a definitional bias associated with dominant forms of masculinity.

30. Brown and Pytlak (2020), op. cit., pp 9-10.

31. Criado-Perez, Caroline, *Invisible Women: Exposing Data Bias in a World Designed for Men* (London: Penguin Vintage, 2019); D'Ignazio, Catherine and Lauren F. Klein, *Data Feminism*. (Boston: MIT press, 2020).

32. See: Chin, Caitlin and Mishaela Robison, 'How AI bots and voice assistants reinforce gender bias', Brookings Institute (23 November 2020). https://www.brookings.edu/research/how-ai-bots-and-voice-assistants-reinforce-gender-bias/; on voice assistants and race, see Moran, T.C., 'Racial technological bias and the white, feminine voice of AI VAs, *Communication and Critical/Cultural Studies*, 18(1) (2021), pp. 19-36. See also West, Mark, Rebecca Kraut, and Chew Han Ei, *I'd Blush If I Could: Closing gender divides in digital skills through education* (UNESCO, 2019). https://en.unesco.org/Id-blush-if-I-could

33. Stark, Luke, 'Facial Recognition is the Plutonium of AI', XRDS – Crosswords (ACM) (April 2019). https://xrds.acm.org/article.cfm?aid=3313129; Keyes, Os, 'Counting the Countless: Why data science is a profound threat for queer people', *Real Life*, (8 April 2019); Bacchini, Fabio and Ludovica Lorusso, 'Race, again: how face recognition technology reinforces racial discrimination', *Journal of Information, Communication and Ethics in Society*, vol. 17, no. 3 (2019), pp. 321-335; Kosinski, Michal and Yilun Wang 'Deep neural networks are more accurate than humans at detecting sexual orientation from facial images', *Journal of Personality and Social Psychology*, 114(2) (2018), p. 246; Wilkinson, Phillip H.C., 'The Legal Implications of Sexual Orientation-Detecting Facial Recognition Technology', Dukeminier Awards: Best Sexual Orientation Law Review Articles, [s. l.], v. 20 (2021), pp. 301–342.

34. Slupska, Julia, 'Safe at home: Towards a feminist critique of cybersecurity', *St Anthony's International Review*, 15(1) (2019), pp. 83-100; Slupska, Julia and Leonie Maria Tanczer, 'Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things. In *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing Limited, 2021).

A broad understanding of cybersecurity also captures the online abuse of women, girls, and people of diverse gender identities, expressions, and sexual orientations referred to as 'online violence against women and girls' or, more commonly and inclusively, '**online gender-based violence**'. People of all genders, for instance, may be targeted by the non-consensual circulation of intimate images ('revenge porn'), which then interact with patriarchal and heteronormative gender biases to produce patterns of stigmatization and discrimination for women, girls, and people of diverse gender identities, expressions, and sexualities.[35] Similarly, people of all genders (particularly, according to some studies, people of diverse gender identities, expressions, and sexualities) are vulnerable to blackmail following the solicitation (or hacking) of intimate images (a form of 'sextortion').[36] The Internet can also be used to facilitate sexual violence and exploitation in the form of human trafficking and the circulation of child sexual abuse material.[37]

The Internet is also a means of circulation for extremist, racist, misogynistic, homophobic, and transphobic content.[38] This content facilitates violence against women, girls, and people of diverse gender identities, expressions, and sexual orientations, as well as marginalized peoples, both on and offline. It can also serve as a form of recruitment for young people,[39] exposing them to a range of threats, from sexual exploitation to participation in violence to engagement with the criminal justice system.

Finally, women, girls, and people of diverse gender identities and expressions are often targeted by misogynistic, homophobic, and transphobic (as well as, often, racist, fatphobic, and ableist) hate speech and online harassment that significantly impact their ability to equitably access the Internet and social media.[40] As the Internet forms a key part of the public sphere for all democracies, this is a substantial threat to human rights. Studies have also shown that women politicians, particularly those of minoritized communities, are disproportionately likely to receive threats and online harassment, producing a disincentive to women's participation in politics that, again, significantly harms the functioning of democracy.[41]

In sum, incorporating gender equality into cybersecurity governance requires a recognition that individual citizens (particularly but not exclusively women, girls, and people of diverse gender identities and expressions), as well as civil society and groups representing women and people of diverse gender identities, expressions, and sexualities, have a need for, and a right to, cybersecurity – including the state resources needed to provide it. It also requires mainstreaming gender analysis into all forms of cybersecurity governance and practice, including those that do not seem to be immediately 'about'

35. See, for example, Plaha, Monica et al., 'Inside the secret world of trading nudes', BBC News (22 August 2022). https://www.bbc.co.uk/news/uk-62564028

36. Powell, Anastasia and Nicola Henry, 'Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults, *Journal of Interpersonal Violence*, 34(17) (2019), pp. 3637-3665; Gámez-Guadix, Manuel and Daniel Incera, 'Homophobia is online: Sexual victimization and risks on the internet and mental health among bisexual, homosexual, pansexual, asexual, and queer adolescents', *Computers in Human Behavior*, 119 (2021), 106728.

37. See Sharland et al. (2021), op. cit., p. 24.

38. Shaw, Adrienne, 'The Internet is Full of Jerks, Because the World is Full of Jerks: What Feminist Theory Teaches Us About the Internet', *Communication and Critical/Cultural Studies*,11(3) (2014), pp. 273-277; see also UN Human Rights Council Report, *Recommendations made by the Forum on Minority Issues at its thirteenth session on the theme "Hate speech, social media and minorities": report by the Special Rapporteur on Minority Issues, Fernand de Varennes*, A/HRC/46/58. https://digitallibrary.un.org/record/3901780?ln=en; Plan International, *Free to be Online?*, (Plan International, 2020). https://plan-international.org/publications/free-to-be-online/; Marston, Kate, 'Researching LGBT+ youth intimacies and social media: The strengths and limitations of participant-led visual methods', *Qualitative Inquiry* 25, no. 3 (2019), pp. 278-288; Powell, Anastasia, Adrian J. Scott, and Nicola Henry, 'Digital harassment and abuse: Experiences of sexuality and gender minority adults', *European Journal of Criminology*, 17(2) (2020), pp. 199–223.

39. See, for instance, Sharland et al. (2021), op. cit., pp. 27-8; for regionally disaggregated details, see: Alava, Séraphin, Divina Frau-Meigs, and Ghayda Hassan, *Youth and Violent Extremism on Social Media: Mapping the research*, (UNESCO Publishing, 2017); Hassan, Ghayda et al., 'Exposure to extremist online content could lead to violent radicalization: A systematic review of empirical evidence', *International Journal of Developmental Science*,12(1-2) (2018), pp. 71-88.

40. Gámez-Guadix and Incera (2021), op. cit.; Powell and Henry (2019), op. cit.;

41. See Di Meco, Lucina and Saskia Brechenmacher, 'Tackling Online Abuse and Disinformation Targeting Women in Politics', Carnegie Endowment for International Peace (30 November 2020). https://carnegieendowment.org/2020/11/30/tackling-online-abuse-and-disinformation-targeting-women-in-politics-pub-83331; Amnesty International UK, 'Black and Asian women MPs abused more online'. https://www.amnesty.org.uk/online-violence-women-mps; and Inter-Parliamentary Union, 'Sexism, harassment, and violence against women parliamentarians' (IPU, 2016). https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians

gender (or conventional definitions of security). It also, of course, requires gender parity in all aspects of cybersecurity governance, including enforcement, implementation, and oversight. This broader scope of cybersecurity, along both state/individual and system/society axes, is summarized in Table 1.

Table 1: Gender and the scope of cybersecurity

	Systems and networks	Broader digital society
State/ corporate	*(Conventional definition)* ❖ Prioritizes supposedly masculine activities ❖ Gender-blind rather than gender-neutral ❖ Individuals considered as security risk (human factor, social engineering, or 'weakest link') ❖ Tendency to dichotomize (state) security against privacy	❖ Disinformation as political or societal threat ❖ Electoral interference as cybersecurity issue ❖ Corporations concerned with online reputation ❖ Individuals considered as sources or naive consumers of dis/misinformation ❖ Tendency to dichotomize (state) security against privacy
Individual/ human-centric	❖ Individuals considered as targets and victims of cyber operations rather than risk factors ❖ Includes gendered and intersectional experiences of cyber operations ❖ But still involves gendered privileging of systems over people, artificially narrowing scope of security threats	***(Recommended definition)*** ❖ **Security threats based on experiences of most vulnerable in society** ❖ **Includes wide range of gendered harms online and connected to digital technologies** ❖ **Incorporates privacy as fundamental aspect of rather than alternative to security**

4. Cybersecurity, gender, and the principles of good security sector governance

A sound approach to cybersecurity is based on the principles of good security sector governance: security needs to be delivered in a transparent, effective, and accountable manner, as a public good and responding to the security needs of all citizens.[42] Gender equality – equality of men, women, and people of diverse gender identities and expressions – is essential to an open, safe, and functioning cybersphere and its governance, and to democracy as a whole. All good governance principles thus have gender equality as an integral component: it is impossible to implement them without it.

Table 2: Principles of good security sector governance[43]

❖ Effectiveness	❖ Responsiveness	❖ Accountability	❖ Rule of law
❖ Efficiency	❖ Participation	❖ Transparency	

Effectiveness in cybersecurity governance cannot be achieved without understanding that both cybersecurity threats and policy frameworks affect genders in different ways

Effectiveness in cybersecurity governance cannot be achieved without understanding that both cybersecurity threats and policy frameworks affect genders in different ways. The standard of effectiveness for cybersecurity policies should be mitigating the negative consequences of online participation and digital technologies for all genders (the recommended definition in Table 1). This can only be attained by ensuring that policy frameworks and technical solutions, firstly, use gender analysis to identify the gendered effects of cybersecurity threats on women, men, and people of diverse gender identities and expressions and, secondly, address these effects in a meaningful, gender-responsive way. While a standard of effectiveness based on a narrower conventional scope of cybersecurity (Table 1) might be attractive in the short term, in the long term it erodes key principles of democracy, including maintaining trust in society and upholding the fundamental rights of citizens.

Digital technologies have the potential to significantly improve the **efficiency** of security governance by helping institutions to make the best possible use of public resources in fulfilling their respective roles, responsibilities, and missions. In general, good cybersecurity governance contributes to this aim by reducing the vulnerabilities and risks associated with widespread digital adoption. For example, many state security organizations now depend on complex layers of digital databases, communications, and analysis tools, which offer a large 'attack surface' for malicious cyber actors. Improving the cybersecurity of these organizations is necessary to ensure that such digitalization efforts improve the efficient functioning of the security sector, rather than expose it to new and potentially catastrophic risks.

However, a gender-blind approach to cybersecurity governance can introduce, rather than reduce, inefficiency, by preventing institutions from drawing on and incorporating diverse experiences, capabilities, and roles. Furthermore, given the interconnectedness and transferability of cybersecurity threats, gender-blind cybersecurity governance obscures the full range of harms potentially associated with digital

technologies. Software used for gender-based coercive control today could be a state national security threat tomorrow, and vice versa. In this way, failing to recognize gendered dimensions of governance and to address the needs of all genders introduces significant inefficiency to cybersecurity governance and, consequently, to security governance more broadly.

This notion of efficiency also directly relates to the principle of **responsiveness** in good governance. Cybersecurity policies and technological solutions should also address the core of the problem of inequality and empower women, men, and people of diverse gender identities and expressions by creating a safe online environment. This will not be possible without equal **participation** of all genders in cybersecurity policymaking and in the development of technical standards. Prioritizing gender equality in cybersecurity governance, in turn, promotes the equal participation of people of all genders in politics and public life. Gender-equal cybersecurity governance is therefore indispensable for the meaningful functioning of democracy.

Gender equality is also central to the **accountability** and **transparency** principles of good governance in cybersecurity. True accountability can only be secured through eliminating barriers for all genders to be equally and meaningfully involved in the oversight of the development and enforcement of cybersecurity policies and frameworks. It also requires mechanisms to meaningfully address gender, sexual, and other intersectional inequalities in cybersecurity technology, practices, or governance once they are identified. The participation of CSOs, including but not limited to women's organizations, human rights groups, LGBTQI+ advocates, privacy organizations, migrants' rights groups, and privacy advocates, in cybersecurity governance is therefore key to good governance. Transparency ensures that gender inequalities can be identified and tackled.

Finally, gender equality is indispensable to **the rule of law**. By its very nature, the rule of law principle guarantees equal protection of human rights for all genders and helps to secure equal access to justice and other remedies. It is also a crucial instrument in mitigating the negative consequences of cybersecurity threats or gendered effects of cybersecurity policies. All other principles must be rooted in the rule of law as one of the cornerstones of democracy.

5. Cybersecurity challenges to the principles of good security governance

The integral role of gender equality in the principles of good cybersecurity governance outlined above could equally be applied to many other areas of security governance.[44] However, cybersecurity presents three unique challenges to these principles.

Cybersecurity governance is fundamentally multistakeholder

While multistakeholder or polycentric governance is a feature of many issue areas, both in security and more broadly, cybersecurity requires multistakeholder governance to an unusual degree. First, Internet governance itself is explicitly based on a multistakeholder model, with non-governmental entities in

44. See DCAF, OSCE/ODIHR, and UN Women, *Gender and Security Sector Reform Toolkit* (Geneva: DCAF, 2008). https://www.dcaf.ch/gender-and-security-toolkit

technical communities, civil society, and the private sector not only acting as inputs to Internet – and therefore cybersecurity – policy, but owning and operating key parts of the technical infrastructure, from cables to routing protocols to emergency response. The multistakeholder nature of cybersecurity governance makes **effectiveness** challenging, as many parties must agree on security policies and their implementation. This raises the risk that a gender-blind definition of cybersecurity, and associated policies, will emerge as the consensus definition. While multistakeholder governance is, by definition, more focused on inclusive participation than alternatives, in cybersecurity such participation can still be skewed by geographic location, digital literacy, and specific technological skills. It is, in other words, a more complex challenge for incorporating intersectionality (gender, sexuality, class, race, disability, location, and so on) into cybersecurity governance and policy assessment.

Cybersecurity governance is highly dependent on large multinational private companies

As part of a wider multistakeholder governance architecture, large multinational private companies have an extraordinary impact on the cybersecurity landscape. This includes social media platforms underpinning the online interactions of billions of individuals, large software companies owning and operating systems used by nearly all computers, or even integrated technology companies with stakes in everything from Internet cables to online commerce, cloud computing, and mobile applications. Such dependence poses challenges for **accountability**, as these private companies have little democratic oversight even in their country of headquarters, and effectively zero elsewhere. These companies often do not themselves prioritize gender equality and do not have gender parity across positions and levels of seniority. This extends challenges of good gender cybersecurity governance into the private sector. These actors also have little incentive to be **responsive** to particular issues, needs, and rights, including those of gender and sexual equality, those especially relevant to marginalized communities, or those championed by women's and LGBTQI+ activist and advocacy groups. Instead, corporations tend to create gender-blind security policies that are assumed to be as broadly applicable as possible for cost and resource reasons.[45]

Cybersecurity governance is fast-moving, unpredictable, and innately international

The underlying field of digital technologies changes rapidly, meaning that cybersecurity governance is also fast-moving. The entrepreneurial and innovation-led philosophy of Silicon Valley – 'move fast and break things' – is replicated in the cybersecurity sector, as a highly active industry is constantly evolving to keep up with the latest technological threats. While this is, in principle, good for both **responsiveness** and **efficiency** as principles of good governance, in practice such constant optimization is nearly always focused on increasing profit or bringing a new product to market rather than protecting rights, including gender equality, or achieving social or democratic aims (such as the equal and safe participation of people of all genders in public life). The speed of digital change also makes it challenging to effectively identify intersectional challenges to gender and cybersecurity – wherein technologies or policies may have unintentional externalities for specific, often marginalized, social groups.

The fast-moving nature of the sector also makes cybersecurity governance unstable, subject to repeated leaks, scandals, and serious incidents. This instability makes cybersecurity governance relatively **transparent** compared with other security sectors, at least in terms of public access to information about

45. This challenge associated with private companies is noticeably not present in global non-profit organizations governing the unique identifiers and developing Internet protocols, which have robust processes for including a variety of stakeholders. However, such organizations still face the wider challenges of multistakeholder governance noted above.

cybersecurity events and issues. However, such chaotic transparency is limited, rarely including, for example, the ability to scrutinize or evaluate algorithmic or automated decision-making with significant impacts on individual people. Given the gendered biases in large data sets, models, and algorithms mentioned above, this has the potential to compound gender inequalities without robust procedures and standards for ongoing gender analysis. Finally, cybersecurity is global in a way that few security sectors can match, with threats and incidents crossing borders almost instantaneously. This poses challenges for the **rule of law**, as multiple jurisdictions are involved in any cybersecurity or cybercrime case. This can increase the challenges faced by victims of all genders – but particularly women and people of diverse gender identities and expressions – in accessing justice.

6. How gender equality addresses cybersecurity challenges to good security sector governance

As already outlined in this paper, a focus on gender equality advocates for expanding the scope of cybersecurity governance to include all relevant actors and rights (as in section 3 above, albeit recognizing that wider definitions are more difficult to operationalize and keep coherent). The current narrowness and lack of consensus on the scope of cybersecurity (as described in section 3) constitute a barrier to gender equality, and so further clarity is necessary. Gender equality also improves cybersecurity governance by reinforcing all the principles of good security sector governance (as detailed in section 4). In this way, it is a normative aim in itself, and so gender mainstreaming should be applied to all aspects of cybersecurity governance. Finally, in addition, gender equality also helps address the cybersecurity-specific challenges identified in section 5, as follows.

Including gender and intersectional equality in multistakeholder models of governance

The multistakeholder model of governance, by definition, relies on the idea of consensus-driven policies developed with input from various stakeholder groups following the principle of equal footing.[46] This principle is based on the formal recognition of the need for equal input from all stakeholder groups based on sectors, such as governments, the private sector, the technical community, and academia. Yet, as long as there is still a comparative lack of participation and representation of women and people of diverse gender identities and expressions in cybersecurity governance, especially in technical fields, multistakeholder models will not be able to take into account the gendered dimensions of cybersecurity, let alone address them in a meaningful way, recognizing the needs of all genders. CSOs representing the concerns and capacities of diverse women and people of diverse gender identities, expressions, and sexual orientations therefore not only have the right to participate in cybersecurity governance but can also help to improve its efficacy in providing individual security and supporting democracy.

Gender equality considerations help to shift the focus from what is currently considered as equality of input based on the notion of stakeholder groups to recognizing that meaningful interpretation of the principle of equal footing requires ensuring gender equality and intersectional consideration within these groups. As part of the broader issue of participation and representation, stakeholders must also address the gendered hierarchy of prestige and priorities that elevates technical expertise and input over other

46 Doria, Avri, 'Use [and Abuse] of Multistakeholderism in the Internet'. In: Radu, R., J.M. Chenou, and R. Weber (eds), The Evolution of Global Internet Governance (Berlin, Heidelberg: Springer, 2014), p. 116.

forms of participation in cybersecurity governance, as opposed to policymaking, oversight, and evaluation.

Advocating for good corporate governance

The private sector plays a significant role in providing cybersecurity, not only by securing infrastructure and networks but also by developing organizational policy and technology in a manner that recognizes the potential for misuse and abuse of legitimate or lawful technologies – including those outside the traditional security sector – to exacerbate existing patterns of gendered and sexual inequality and facilitate GBV. Issues like gendered bias in algorithms, gendered effects of the misuse of certain devices and technologies, such as location and health tracking apps, the gendered harms of access to and use of users' data, including sharing data with third parties, must be addressed as much by the private sector as by (inter)governmental regulatory or legal frameworks.

A focus on gender equality can help to recognize and enhance the role and responsibilities of the private sector in ensuring responsiveness to the cybersecurity needs and concerns of all genders. This can be achieved via commitments and efforts made under current frameworks for corporate social responsibility, expanding commitments to gender, sexual, and racial equality and inclusion, as well as to combatting GBV.[47]

Helping to preserve and protect the rule of law

Gender equality is crucial in reinforcing the rule of law, as one of the cornerstone principles of good governance in cybersecurity. This reinforcement goes beyond providing equal access to justice and mechanisms for redress. Many cybersecurity and cybercrime laws are still framed as 'gender-neutral', relying on incorrect assumptions of equal protection for an abstract 'citizen' from crime and other threats, independent of gender. These laws are, however, gender-blind, as cybersecurity cannot be achieved without accounting for the diversity of experiences, needs, capacities, and vulnerabilities of people of all gender identities. Focusing on gender and intersectional equality helps to avoid homogenization and the inadvertent externalities that often arise as a result of legal frameworks: for example, when laws intended to protect women online are used to suppress women's groups, journalists, or LGBTQI+ persons. Gender mainstreaming can also guide lawmakers in balancing a complex array of rights, such as protection from gender-based online harassment with freedom of expression.[48] While further exploration of this topic is beyond the scope of this paper, it deserves separate consideration in the context of security sector governance.

47 Such corporate commitments could usefully draw on the International Labour Organization (ILO)'s Convention 190 (which came into force in 2021), which 'recognizes the right of everyone to a world of work free from violence and harassment, including gender-based violence and harassment'. ILO, *Eliminating Violence and Harassment in the World of Work*. https://www.ilo.org/global/topics/violence-harassment/lang--en/index.htm

48. See, for example, OHCHR, 'Gender equality in freedom of expression remains a distant goal – UN expert', press release (OHCHR, 18 October 2021). https://www.ohchr.org/en/press-releases/2021/10/gender-equality-freedom-expression-remains-distant-goal-un-expert. For instance, legislation ostensibly intended to protect women and girls from online harassment has been used in some contexts to suppress speech by women journalists and human rights defenders, as well as expressions of feminism and/or LGBTQI+ identities; for examples of this, see Human Rights Watch, 'Online Harassment of Women in Pakistan' (22 October 2020). https://www.hrw.org/news/2020/10/22/online-harassment-women-pakistan; 'Egypt: Spate of "Morality" Prosecutions of Women' (17 August 2020). https://www.hrw.org/news/2020/08/17/egypt-spate-morality-prosecutions-women; and 'Abuse of Cybercrime Measures Taints UN Talks' (5 May 2021). https://www.hrw.org/news/2021/05/05/abuse-cybercrime-measures-taints-un-talks

CONCLUSION

To conclude, the following table summarizes the relationship between the principles of good security governance, cybersecurity challenges for these principles, and gender policy recommendations to address these challenges and enhance the principles of good governance for cybersecurity. These recommendations are drawn from the analysis across all preceding sections of this paper.

Table 3: Principles of good governance, cybersecurity, and gender

Good governance principle	Cybersecurity challenges	Gender policy recommendations
Effectiveness	Multistakeholder coordination is based on the principle of equal footing rather than representation.	Ensure capacity and resources within multistakeholder governance institutions to promote and support gender equality, including gender experts and champions. Involve key CSOs, including women's and LGBTQI+ groups in consultations on policy design, implementation, and oversight.
Efficiency	Cybersecurity actors focus on narrow concepts of economic or technological optimization.	Ensure that economic analyses of cybersecurity threats and risks include gender-sensitive accounts of labour, profit, and gross domestic product (GDP) and actively work to redress gendered inequities. Ensure that efficiency concerns in cybersecurity are not prioritized over gender equality.
Responsiveness	Narrow state-centric definitions of cybersecurity omit many gendered threats and harms. Private sector adoption of global, automated systems for cybersecurity and content moderation lacks community engagement or sensitivity.	Consult on the appropriate scope of cybersecurity to form the basis for efforts towards security sector reform and good governance, from an intersectional gender perspective. Analyse and address, based on the collection of sex-disaggregated data, the gendered effects and harms of potential misuse of technologies and products. Ensure that data collection is sensitive to gender diversity (that is, not presuming a gender binary).

Good governance principle	Cybersecurity challenges	Gender policy recommendations
Participation	A gendered hierarchy of prestige and priority elevates technical expertise and input over other forms of participation.	Build capacity to ensure meaningful participation of all gender identities in cybersecurity policymaking. Promote and compensate people in all cybersecurity roles equally to avoid devaluing of non-technical knowledge. Provide mentoring, technical training, and job design to support women and LGBTQI+ people to succeed in technical cybersecurity roles. Provide resources to support women's, LGBTQI+, and other relevant CSOs in governance.
Accountability	Democratic oversight of large technology companies is challenging.	Maintain an open and participatory democratic process, focused on oversight of gendered aspects of corporate governance. Use public-private partnerships and state contracts to encourage corporations to prioritize gender equality in workforce and in technology/ product design.
Transparency	Transparency depends on chaotic, unpredictable leaks, and underlying code and algorithms are rarely subject to scrutiny.	Support public scrutiny and input from non-commercial parties, such as civil society and academia, to provide structure to and strengthen transparency around cybersecurity technologies and policies. Provide technical training on algorithms and digital governance, including information on gender, sexual, and racial bias, to legislators overseeing cybersecurity.

DCAF Geneva Centre for Security Sector Governance

DCAF – Geneva Centre for Security Sector Governance

Maison de la Paix, Chemin Eugène-Rigot 2E | CH-1202, Geneva, Switzerland

Tel: +41 22 730 94 00 | Email: info@dcaf.ch | Twitter @DCAF_Geneva