APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

A FRAMEWORK FOR DEVELOPING GENDER-RESPONSIVE CYBERSECURITY POLICY

LITERATURE REVIEW

A framework for developing gender-responsive cybersecurity policy: Literature review

This publication was developed and produced by APC.
External researcher Paz Peña was the author.

Coordination and editing: Verónica Ferrari and Paula Martins (APC)

Editorial support: Gaurav Jain (APC)

Copy editing: Sugandhi Ravindranathan

Proofreading: Lori Nordstrom (APC)

Design and layout: Cathy Chen (APC)

Published by APC 2022

ISBN 978-92-95113-55-8
APC-202212-GAPS-R-EN-DIGITAL-345

This publication was developed with support from the UK Government.

I. INTRODUCTION

Beyond the fact that cybersecurity problems are formulated in techno-functional terms, which gives it an objective halo, cybersecurity is a contested field.[1] As Deibert notes, cyberspace has no fixed properties in time and space, making it an inherently political field: it is a contest between different worldviews, ideologies and strategic interests, even if all these are concealed as unquestioned assumptions.[2] Indeed, security, as a value, is not universal and immutable; instead, security is constantly sustained and elaborated by local socio-cultural practices that characterise who and what is considered "safe" or "unsafe", conceptualising the objects that are protected by security and articulating the moral justification for security.[3] Driven by motley theoretical currents such as Science and Technology Studies (STS), Human-Computer Interaction (HCI) or the Women, Peace and Security (WPS) Agenda, among others, the gender approach, on the one hand, like the theoretical currents of feminism and intersectionality, has also entered the dispute about what and how cybersecurity is considered. And while there is no cogent theoretical body that develops the cybersecurity proposition from these approaches, this document intends to explore how these perspectives have been deployed in cybersecurity and what elements appear to be cross-cutting. This document is a part of a framework developed by the Association for Progressive Communications that seeks to support policy makers and civil society organisations by providing practical guidance for developing gender-responsive cybersecurity policies, laws and strategies. Thus, it is expected to contribute to the various stakeholders interested in the contributions of a gender approach to cybersecurity to find a theoretical background that can support their policies and actions.

This paper is organised as follows: first, a short positioning on important concepts around gender. Second, it describes the general background context that precedes the idea of cybersecurity as a gendered space. The third part explores the connections between the irruption of human rights in cybersecurity and the gender perspective and analyses the most prevalent crosscutting concepts that appear in the different research that takes gender into the various fields of cybersecurity. In the fourth part, some of the topics where the gender perspective in cybersecurity is more present are discussed in depth, to end with a brief chapter of conclusions.

1. Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7,* 61-73. https://doi.org/10.1007/s10676-005-4582-3; Deibert, R. (2018a). Trajectories for future cybersecurity research. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security*; Slupska, J. (2019). Safe at Home: Towards a feminist critique of cybersecurity. St. Anthony's International Review, 15. https://ssrn.com/abstract=3429851
2. Deibert, R. (2018a). Op. cit.
3. Nissenbaum, H. (2005). Op. cit.

II. IMPORTANT CONCEPTS

This literature review draws on diverse research and theoretical currents that do not necessarily clarify their perspective on feminism and the gender approach; concepts which, although related, are slightly different. Some of them use gender approach and feminism indistinctively, others seem to refer to gender analysis as a technical realm of feminism, some seem to view gender only as a demographic factor, and many of them respond to the aim of gender mainstreaming as a strategy for the promotion of gender equality in all societal spheres. At the same time, for some of them, gender equals only women, while others are explicit about the diversity of identities behind this concept.

Because of this difficulty and considering the general aim of undertaking a review of how gender has been considered up until now in cybersecurity, this paper does not make significant distinctions between these related notions. However, it respects the concepts raised initially (it does not replace gender with feminism, for example) and only raises alerts when gender considerations seem to move away from what we understand by gender analysis and feminism. But what do we mean by these concepts? It seems, then, important to make a very general conceptual elaboration of ideas that will be repeated in the text.

Gender: The set of ideas, representations, practices and social prescriptions elaborated based on the anatomical difference between the sexes. But gender is more than a powerful principle of social differentiation: it is a brutal producer of discrimination and inequalities. The ideas and practices of gender hierarchise human beings socially, economically and legally.

Gender approach or gender analysis: A tool to analyse gender differences and mitigate them. Gender is not just about the difference between the sexes but also about power. Therefore, any convincing analysis of the gender order will need to combine the study of gender difference with an account of gender power. This approach can only analytically and strategically influence certain public policies and governmental actions but does not aim to open new political perspectives.

Feminism: Feminism is a diverse and interdisciplinary approach to issues of equality and equity based on gender, gender expression, gender identity, sex and sexuality, as understood through critical social theories and political activism.

Gender mainstreaming: The process of assessing the implications for women and men of any planned action, including legislation, policies or programmes, in all areas and at all levels. Its ultimate goal is to achieve gender equality.

Intersectional perspective: The intersectional perspective identifies a system of diverse oppressions – among which is gender, but which also includes race, religion and social class, among others – that hierarchises a person in society, shedding light on other differences that constitute people's identity and enriching the notion of the subject that, until then in feminism, was perceived only from its gender; with intersectionality, multiple subjects emerge, traversed by diverse attributes. Thus, social problems have become more complex since the analysis now considers multiple power systems that were seen separately until then.[4]

4. Collins, P. (2019). *Intersectionality as Critical Social Theory*. Duke University Press.

III. BACKGROUND OF CYBERSECURITY AS A GENDERED SPACE

There is a general agreement that gender in cybersecurity has been largely absent from cybersecurity discussions as it is still considered a "secondary issue" today.[5] But just because it is absent from the conversations does not mean it does not exist or that cybersecurity is in any way gender-neutral. In fact, research shows that cybersecurity, in its broader conception, is a gendered space, affecting how it is conceived and deployed in its different fields and stages; more specifically, it is pointed out that the logic of hegemonic masculinity found in both the security and technology fields influences cybersecurity practices.[6]

On the one hand, the security field can be considered a gendered institution because gender differences are very present or marked. As Myrttinen notes, "hard" security and related institutions and activities (e.g. the military) are seen as masculine in that ("real") men do them and they "can only be done well by men."[7] In contrast, "soft" security (e.g. peace building, health care delivery) is associated with femininity. Therefore, its structure, practices, values, rites and rituals reflect accepted notions of masculinity and femininity and, in turn, it is an institution that helps to create gender identities.[8] In this context, cybersecurity is still highly related to the military branch, so the latter's gender patterns tend to be repeated in cybersecurity also.[9]

Likewise, different traditions of feminist analysis have sought to denaturalise the relations with technology attributed to gender. It has been argued that the symbolic representation of technology is strongly influenced by gender, to such an extent that the affinity with technology in Western societies is now seen as an integral and constitutive part of both the hegemonic male gender identity and the culture of technology, which ends up creating a circle in which more men work in the field, so they are the ones who produce more technology.[10] Beyond the specific context of cybersecurity, technology design is gendered: it misconstrues, omits and consolidates specific gendered usages, privileges practices perceived as masculine over feminine, and stereotypes femininity in problematic ways.[11] These aspects of gender directly impact cybersecurity.

5. Pytlak, A. (2021). Bringing gender analysis into international cybersecurity. *Cyber Peace & Security Monitor, 1*(8). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.8.pdf; Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03; Shoker, S. (2021). *Making gender visible in digital ICTs and international security*. Report submitted to Global Affairs Canada. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/research-canada-1.pdf
6. Nieminen, L. (2021). *Why is human trafficking excluded from the EU's cybersecurity?: An explorative study about cybersecurity and human trafficking in the European Union*. http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9698
7. Myrttinen, H. (2020). *Tool 1: Security Sector Governance, Security Sector Reform and Gender*. DCAF, OSCE/ODIHR & UN Women. https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender
8. Barrett, F. J. (1996). The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy. *Gender, Work & Organisation, 3*(3), 129-142. https://doi.org/10.1111/j.1468-0432.1996.tb00054.x
9. D'Hondt, K. (2016). *Women and Cybersecurity*. Master's thesis, Harvard Kennedy School. Nieminen, L. (2021). Op. cit.
10. Wajcman, J. (2000). Reflections on Gender and Technology Studies: In What State is the Art? *Social Studies of Science, 30*(3), 447-464. https://doi.org/10.1177/030631200030003005
11. Millar, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: Design, defence and response*. United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

IV. CYBERSECURITY CONCEPTS: TENSIONS FROM A GENDER PERSPECTIVE

For Dunn Cavelty, two different ways of understanding cyber technologies prevail in society. The first sees cybersecurity as the practice of fixing broken objects, and the second sees it as a tool to promote political goals.[12] In Reid and van Niekerk's conceptualisation,[13] we move from an information security approach (which seeks to protect existing computer systems and networks from hostile action in an exclusively organisational context) to a broader cybersecurity approach, which is more responsive to the massification of the use of digital technologies. In cybersecurity, it is understood that technologies create vulnerabilities that can have detrimental effects on society so that "threatening" actors come to the fore, and a link is established with the abstract notion of "national security". States are the actors called upon to restore control over the misuse of cyber technologies through a more coordinated and focused effort from the national and international society, governments and the private sector. In this context, cyberspace is defined as a complex environment resulting from the interaction of people, software and services on the internet through technological devices and networks connected to it. And cybersecurity, then, involves protecting the interests of a person, society or nation, including their information-based and non-information-based assets that need to be protected from risks related to their interaction with cyberspace.[14]

But tensions and controversies in defining cybersecurity unfold when one must determine the "referent object" of security.[15] A fundamental approach in which the gendered perspective of cybersecurity is anchored is the human-centric approach. This strategy, instead of prioritising the territorial sovereignty of networks, places human beings – regardless of their nationality or citizenship – as the main objects of security, whereby networks are seen as part of the essential basis for the modern exercise of human rights, such as access to information, freedom of thought and freedom of association.[16] This approach differs from national security approaches that conceptualise the state, infrastructures and institutions as the focus of cybersecurity threats. It may also differ from private sector approaches in which humans are reduced to network nodes necessary to maximise profit.[17]

Discussions on the human-centred approach to cybersecurity have highlighted the importance of international human rights law as a basis and framework for cybersecurity. There is a consensus about the application of international law to cyberspace, with its norms applying fully and without distinction. However, some rights are particularly relevant in cyberspace, as they are closely linked to information in its various aspects and manifestations; for instance, privacy and freedom of expression and information complement the right to security, personal

12. Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance,* 6(2), 22-30. https://www.cogitatiopress.com/politicsandgovernance/article/download/1385/1385
13. Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Information Security for South Africa 2014.* https://ieeexplore.ieee.org/document/6950492
14. Ibid.; Slupska, J. (2019). Op. cit.
15. Slupska, J. (2019). Op. cit.; Dunn Cavelty, M. (2014). Op. cit.; Brown, D., & Esterhuysen, A. (2019, 28 November). Why cybersecurity is a human rights issue, and it is time to start treating it like one. *APC.* https://www.apc.org/en/node/35879
16. Deibert, R. (2018b). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32*(4), 411-424. https://doi.org/10.1017/S0892679418000618
17. Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: The role of civil society. *Journal of Cyber Policy, 6*(3), 375-393. https://doi.org/10.1080/23738871.2021.1909090

freedom and non-discrimination.[18] Thus, the danger of "cyber insecurity" should never be a pretext for violating human rights, with the protection of human rights being at the heart of developing any cybersecurity policy.[19]

In this context, the question from the gender approach is to what extent cybersecurity assumes the power systems that socially hierarchise human beings, both at the level of strategy design and the effects of attacks. In this sense, "feminist cybersecurity", as Slupska puts it,[20] is a questioning approach: for whom are these technologies made? Where can one intervene? What trade-offs are made in technology companies when concerns arise? Whose cybersecurity is cybersecurity? However, although these questions have been increasing in recent years, there is still no complete or agreed conceptualisation of what elements a cybersecurity definition from the gender perspective should encompass. We can, however, highlight some important concepts that different authors emphasise.

Firstly, there is a questioning of the supposed neutrality of cyberspace, which assumes human beings as a neutral universal entity, since, as feminist theoretical currents have denounced, in a hetero-patriarchal and colonial reality, that human being always ends up being a white cis-heterosexual male. On the one hand, this questioning affects the sphere of people's risks and how cybersecurity systems and policies assume these differentiated dangers. Human rights defenders, journalists and people in marginalised or vulnerable situations due to their religion, ethnicity, sexual orientation or gender identity, for example, may experience special risks and suffer consequences from particular threats.[21] As Haciyakupoglu and Wong assert, the assumption that cyberspace is gender-neutral overlooks differences in the capabilities, needs and priorities of different genders and how gender norms condition priorities within cybersecurity designs, where systems are often delineated with the average male user in mind.[22]

As a consequence of the previous point, it seems a vital priority for the gender perspective in cybersecurity to denounce the lack of diversity both in the development of technologies and in the design of cybersecurity strategies and policies. In this sense, an important part of the feminist approach to cybersecurity understands that the production of knowledge of technologies and cybersecurity is inevitably linked to acts of power and assumes that in patriarchal societies where Western scientific epistemology is universalised, women's knowledge is suppressed.[23] Moreover, particularly in cybersecurity, technical expertise is often associated with men and masculinity.[24] In this sense, the call for diversity has to do with the inspiration of the feminist standpoint epistemology, which advocates the revaluation of women's experiences as valid

18. Álvarez, D., & Vera, F. (2017). Ciberseguridad y derechos humanos en América Latina. In A. del Campo (Ed.), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Universidad de Palermo. https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf
19. Brown, D., & Esterhuysen, A. (2019, 28 November). Op. cit.
20. Slupska, J. (2019). Op. cit.
21. Brown, D., & Esterhuysen, A. (2019, 28 November). Op. cit.
22. Haciyakupoglu, G., & Wong, Y. (2021). *Gender, Security and Digital Space: Issues, Policies, and the Way Forward*. S. Rajaratnam School of International Studies. https://www.rsis.edu.sg/rsis-publication/cens/gender-security-and-digital-space-issues-policies-and-the-way-forward
23. Bardzell, S. (2010). Feminist HCI: Taking stock and outlining an agenda for design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. https://doi.org/10.1145/1753326.1753521
24. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.

alternative epistemologies for cybersecurity.[25] This means problematising the lack of intersectional diversity in its broadest sense: from the lack of diverse people working in the industry and developing policies, to the need for a critical look at the methodologies behind cybersecurity.

Thus, on the one hand, it critically reviews cybersecurity models that persist in methodologies that suffer from gender biases and knowledge gaps. According to Julia Slupska, a feminist approach to cybersecurity must be grounded by a focus on harms to humans.[26] Moreover, the challenge of analysing the potential harm to people from cyber attacks is to leave behind the "public versus private" separation made by the traditional stream of cybersecurity focused on national security. Instead, it is also necessary to focus on the micro-level impacts,[27] such as domestic and private spaces, as the latter cannot be assumed only as a security space under the threat of external adversaries.[28] This implies leaving behind a certain elitism of traditional cybersecurity, especially when technology users are qualified only as a "human factor", making them invisible and choosing to focus on more powerful actors such as companies, states or militaries.[29] However, the only way to know what the various threats that can affect people are is to renew threat-modelling practices and focus on citizens' experiences with online threats and how they relate to cybersecurity both as a concept and as a practice.[30] In other words, participatory security design is needed, as this avoids the assumption that the security of the individual will be derived from the security of a technical system and includes the perspective of actors who may generally be marginalised.[31] This is within the trend of thinking distinctly about cybersecurity, and moving from considering people as a problematic and thus excluded layer, to considering humans as part of the solution, recognising the potential they have to contribute to the success of cybersecurity within the broader socio-technical system.[32]

The challenges do not stop there, because once cybersecurity is focused at the micro-level, i.e. in personal security spaces, it is critical to rethink cybersecurity education methodologies. Too often today, technical jargon and victim-blaming are resorted to, i.e. users are reprimanded for choosing weak passwords, clicking on phishing links or sharing nudity.[33] Moreover, methodologies such as "holistic security", widely used by digital security experts

25. Slupska, J., Dawson Duckworth. S., Ma, L., & Neff, G. (2021). Participatory threat modelling: Exploring paths to reconfigure cybersecurity. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411763.3451731
26. Slupska, J. (2019). Op. cit.
27. Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review, 16*(1), 43-48. https://doi.org/10.1080/10402650420002101 48
28. Slupska, J. (2019). Op. cit.
29. Still, an important caveat must be made: calls for the inclusion of domestic and private spaces into cybersecurity frameworks must be careful to justify unwanted intrusions into the lives of minority and lower-class populations since, traditionally, these are the most vulnerable to constant state interventions. See: Slupska, J. (2019). Op. cit.
30. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). *Reconfigure: Feminist Action Research in Cybersecurity*. Reconfigure Network. https://www.oii.ox.ac.uk/news-events/news/reconfigure-feminist-action-research-in-cybersecurity
31. Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (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)*. https://doi.org/10.1145/3368860.3368861; Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.
32. Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005
33. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). Op. cit.

in the field of human rights defenders, are seeking to move away from the machine and be closer to feminist practices of care and self-care. This approach rejects the militaristic security tradition and proposes a care-oriented definition of security as "well-being in action", whereby care means rejecting fear of abstract threats and instead embracing what is imminent and meaningful in people and their own bodies.[34] In addition, education should not only focus on the potential recipients of digital attacks, as this, according to Slupska, makes them responsible for avoiding their misuse:

> Education should also be targeted at abusers and sellers of abuse tools, who bear the primary responsibility for the harm the tools cause. While most purveyors and clients of abuse tools may be beyond persuasion, some may not realise their actions are unethical due to a social environment which is friendly to surveillance practices. Feminist principles of consent and respect for individual autonomy could be incorporated into digital ethics and taught from an early age.[35]

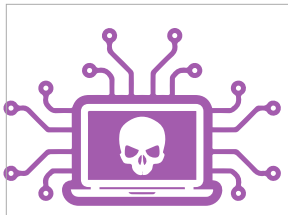
34. Kazansky, B. (2021). 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720985557
35. Slupska, J. (2019). Op. cit.

V. CRITICAL NODES OF CYBERSECURITY FOR A GENDER PERSPECTIVE

In the following section, we identify specific nodes of cybersecurity that gender research has looked at critically. The cross-cutting concepts that we examined above are also deployed in all these nodes. As will be seen, all the nodes are interrelated, so this classification – and, therefore, their separation – is only intended for the referential ordering of bodies of research and more robust evidence.

A) The gender gap in the cybersecurity field

B) The dimensions of gender-based violence in cybersecurity



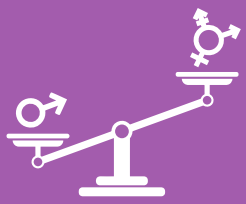
C) Differential vulnerabilities to cyber attacks

D) Differential impact of cyber incidents based on gender

E) Reconfiguring cybersecurity analysis frameworks

F) Feminist autonomous internet infrastructure

G) International public policies on cybersecurity



A) THE GENDER GAP IN THE CYBERSECURITY FIELD

There is a broad consensus that, for some years now, driven by digitisation and the rise of cyber attacks, the global cybersecurity industry has been suffering from a dramatic lack of skilled workers. The current cybersecurity workforce gap stands at more than 3.1 million skilled professionals worldwide, and although the number of industry professionals grew by more than 700,000 in 2020, women still represent only about 25% of the cybersecurity workforce, compared to at least 40% of the global workforce, according to the Pew Research Center.[36]

This problem has been looked at so far from two perspectives: industry and participation in cybersecurity-related policies. Likewise, it seems necessary to emphasise that, although the basis of the problem seems to be the lack of women's participation in these spaces, there is a growing recognition on the one hand that not all women suffer equally from this discrimination and other intersectional crossings are essential to make in the analysis and, on the other hand, that the diversity crisis goes beyond women's participation alone and that other groups historically discriminated against continue to be excluded.

Diversity in the industry

A global qualitative study by (ISC)², published in 2021, concluded that there is a widespread perception that professionals in the cybersecurity industry have a very homogeneous profile: middle-aged white men with more than eight years of experience in an IT or computer-related field.[37] In addition, a systematic problem is identified at both ends of the system that further affects the industry: on the one hand, the incorporation of young women is very slow, and on the other, the lack of diversity is particularly significant in leadership positions. This lack of diversity in cybersecurity teams becomes a vicious circle as it makes working conditions for women in cybersecurity even more difficult. For example, Barsh and Yee highlighted the relationship between the level of diversity in an organisation and the likelihood of females being promoted to senior positions.[38] Likewise, the intense working hours in the masculinised

36. (ISC)². (2021). *In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity.* https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx
37. Ibid.
38. Barsh, J., & Yee, L. (2011). *Unlocking the full potential of women in the US economy*. McKinsey & Company.

culture of cybersecurity is an impractical model for people (more likely to be women) with caregiving responsibilities.[39] Also, bullying and cyberbullying are widespread problems, as shown by a recent study by Respect in Security, which estimates that about one-third of cybersecurity professionals have had personal experiences of online (32%) and in-person (35%) bullying.[40]

Another problem is the lack of diversity related to people's experience and skills.[41] That is, the shortage of diversity relates not only to gender, race or religion but also to the formation of teams with a variety of experiences that can bring a pluralistic culture and innovative approaches to problem solving, as adversaries will exploit the unconscious bias ingrained in the industry by recognising and circumventing the homogeneity of typical security approaches.[42] King-Close argues that as cybersecurity is a new warfare domain that requires new perspectives on problem solving, some of the barriers that have deterred women and other groups from war- and technology-related roles in other fields can be countered.[43] A sign of this is, for example, the growing need to incorporate psychology into cybersecurity analysis, which may be an opportunity for greater diversity, as it is a somewhat feminised career. However, so far, training beyond science, technology, engineering and mathematics (STEM) fields is generally not rewarded in cybersecurity, as most employers consider computer science or engineering training a priority in cybersecurity.[44]

Among the responses to this problem, at the educational level, there is growing evidence of the need for an intersectional look at this low incorporation of women into cybersecurity, particularly concerning their experiences of education in STEM fields when gender is crossed with race and ethnicity.[45] Additionally, at the professional level, the industry is gradually adopting DEI (diversity, equity and inclusion) methodologies to increase diversity within the cybersecurity profession, creating space for respecting biological, demographic or cultural differences, as well as differences in thinking, experience, ability, or leadership style.[46]

Diversity in governance

Gender is a vital determinant of the security risks faced by women, men and people of different gender identities and expressions online and the extent to which they can safely access and use online spaces. Therefore, it becomes imperative to address the lack of participation of women and people of diverse gender identities in cybersecurity provision and governance by incorporating a gender perspective into cybersecurity oversight, provision, and management.[47] However, according to Brown and Pytlak, the participation of women working in

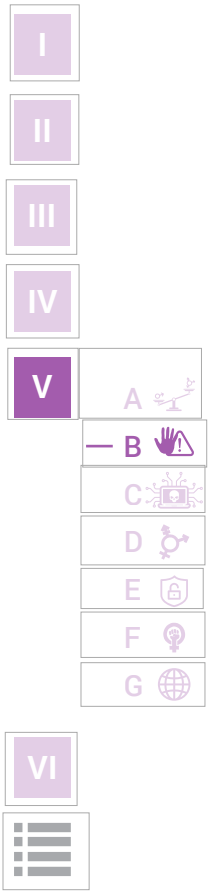
39. D'Hondt, K. (2016). Op. cit.; Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
40. Respect in Security. (2021, 21 July). Over a third of cybersecurity professionals have experienced harassment at industry events. https://respectinsecurity.org/respect-in-security-press-release
41. (ISC)². (2021). Op. cit.
42. Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer, 52*(3), 58-6. https://doi.org/10.1109/MC.2018.2884190
43. King-Close, A. M. (2016). *A gender analysis of cyber war*. Master's thesis, Harvard Extension School.
44. Poster, W. R. (2018, 26 March). Cybersecurity needs women. *Nature*. https://www.nature.com/articles/d41586-018-03327-w
45. Burrell, D. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things, 2*(1). http://dx.doi.org/10.4018/IJHIoT.2018010103
46. (ISC)². (2021). Op. cit.
47. Dorokhova, E., vale, h., Laçí, V., & Mahmutovic, A. (2021). *Cyber violence against women and girls in the Western Balkans: Selected case studies and a cybersecurity governance approach*. The Geneva Centre for Security Sector Governance (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/CyberVAWG_in_WB.pdf

cybersecurity policy and diplomacy has been much less studied than the lack of diversity in the industry, both in its quantitative and qualitative dimensions.[48] For example, an analysis of international cybersecurity negotiations by the United Nations Institute for Disarmament Research (UNIDIR) found that women accounted for only one in five participants, and when states sent a single representative, it almost invariably was a man.[49]

Women's participation in international cybersecurity decision making is important not only as a concrete way to decrease gender inequality, but also in bringing a diversity of perspectives that can allow for more careful handling of information and better policy decisions, including the unique needs that women have in the cybersecurity field.[50] In their research, Brown and Pytlak identify that culturally assigned patriarchal roles influence in different ways the experience of women in cyber politics: from their lack of participation to the constant undermining of their political leadership.[51] In addition, as is common in society, caregiving tasks, which generally fall on women, are again a factor of discrimination. However, for these researchers, the problem of gender diversity is not a "cyber"-unique reality but a broader societal problem that manifests itself as gender inequality in cybersecurity spaces, so addressing it goes hand in hand with more overall changes in the general culture.

48. Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom and the Association for Progressive Communications. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security
49. UNIDIR. (2021). *Fact sheet: Gender in cyber diplomacy*. https://unidir.org/publication/fact-sheet-gender-cyber-diplomacy
50. Sharland, L., et al. (2021). Op. cit.
51. Brown, D., & Pytlak, A. (2020). Op. cit.

B) THE DIMENSIONS OF GENDER-BASED VIOLENCE IN CYBERSECURITY



Much research on gender and cybersecurity comes from studies on gender-based violence and gender inequality in the digital technologies sector.[52] Women and girls face specific cyber threats in the digital age that are considered forms of gender-based violence as they occur because of their gender, or because they disproportionately affect one gender. While this violence is mediated by digital technology, it is part of the same offline structural violence; but its technological dimension adds elements of search, persistence, replicability and scalability that facilitate the aggressors' access to their targets and can exacerbate the harm. Online gender-based violence (OGBV) can manifest itself in various forms and different ways, but it is prevalent for aggressors to use privacy violations as their primary weapon. Thus, for example, as recognised in a report by the UN Special Rapporteur on violence against women, there are attacks such as non-consensual accessing, using, manipulating, disseminating or sharing of private data, information and/or content, photographs and/or videos, including sexualised images, audio clips and/or video clips or "Photoshopped" images.[53] Despite being a growing type of violence with material, psychological and economic consequences for women and society, OGBV is still often disregarded as a problem for cybersecurity due to the sub-estimation of domestic/private issues and the preference to prioritise major threats.[54] This disdain has direct consequences on women and girls, as in addition to OGBV, it also dismisses technology-facilitated intimate violence, online political gender-based violence, and the gender-based violence component of terrorist radicalisation on the internet.

Technology-facilitated abuse by intimate partners (also known as intimate partner abuse, IPA) has a significant difference from other types of OGBV, mainly because aggressors and survivors are not strangers; in fact, they are or have been involved in an intimate relationship that includes a daily coexistence at both online and offline levels. This means that aggressors not only have access to victims and their devices in the physical world but may also have intimate knowledge of them, their routines, habits and preferences.[55] Mainly

52. Ibid.
53. Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*. A/HRC/38/47. https://undocs.org/A/HRC/38/47
54. Slupska, J. (2019). Op. cit.
55. 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*. https://doi.org/10.1145/3322276.3322366

influenced by Human-Computer Interaction (HCI), several authors have begun to investigate the role digital technologies can play in abusive relationships,[56] and, more specifically, the role of the "internet of things" (IoT) and its relationship with IPA and security. The characteristics of digital technologies, including issues such as their usability settings, can be misused, opening avenues for the perpetrator of domestic abuse and intimate partner violence to inflict "techno-abuse", i.e. to surveil, coerce or control another person, making the safety of IoT devices crucial for groups and communities in vulnerable relationships.[57] Likewise, and despite its prevalence in society, IPA is almost wholly ignored in smart home device security analysis research, where device design "mostly assumes that the 'Owner' of the device does not pose a threat to other users of the device. This omission reflects what feminist theorists have long criticised, namely the internal/external binary in which the home is imagined to be a place of safety under threat from external adversaries."[58]

Likewise, and although ICT-mediated gender-based violence often falls below the legal threshold of war, ICTs can be conceptualised as tools that disrupt political life through gender-based violence, but, as in many other policy domains, there is a dearth of systematic data collection on these attacks, both during and outside of government transitions.[59] In this regard, in her 2018 specific report on violence against women in politics,[60] the UN Special Rapporteur on violence against women identifies disinformation by state and non-state actors as a form of online gender-based violence:

> Ultimately, online violence against women in politics is a direct attack on the full participation by women in political and public life and their enjoyment of their human rights. The extent to which such online violence is used by State and non-State actors to spread disinformation aimed at discouraging women from participating in politics, swaying popular support away from politically-active women and influencing how men and women view particular issues has yet to be fully understood.[61]

According to Di Meco, gender disinformation can be defined as the dissemination of misleading or inaccurate information and images against women political leaders, journalists and female public figures, following storylines that are often based on misogyny, as well as gender stereotypes around the role of women.[62] This type of disinformation is designed to alter the public understanding of the trajectory of women politicians for immediate

56. Harris, B. A., & Woodlock, D. (2019). Digital Coercive Control: Insights from two landmark domestic violence studies. *The British Journal of Criminology, 59*(3), 530-550. https://doi.org/10.1093/bjc/azy052; Leitao, R. (2019). Op. cit.; Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Op. cit.; Slupska, J. (2019). Op. cit.; Slupska, J., & Tanczer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In J. Bailey, A. Flynn & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211049
57. Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Op. cit.
58. Slupska, J. (2019). Op. cit.
59. Shoker, S. (2021). Op. cit.
60. Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on violence against women in politics*. A/73/301. https://undocs.org/A/73/301
61. Among the reasons for considering disinformation as a threat to cybersecurity is how data manipulation operations manipulate people's fears and emotions, compromising information security and utilising the cyber infrastructure. See: EU Disinfo Lab. (2021, 24 May). Why Disinformation is a Cybersecurity Threat. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat
62. Di Meco, L. (2020). *Online Threats to Women's Political Participation and The Need for a Multi-Stakeholder, Cohesive Approach to Address Them*. UN Women. EGM/CSW/2021/EP8. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf

political gain and discourage women from seeking political careers. It can come from domestic political adversaries (including state actors) and result from foreign interference, deserving of specific attention due to its nature, volume and impact on democratic processes.

In this context, evidence has been found of state-aligned gender disinformation, in which actors who are part of a state or whose behaviour or interests align with a state engage in gender disinformation to promote political outcomes.[63] Similarly, there is also evidence of gender disinformation employed by foreign state actors to undermine democratic institutions in other countries. For example, a screenshot of a fake Facebook post discussing nudity about Svitlana Zalishchuk, a Ukrainian MP, was amplified by several Russian websites and then actively shared by Ukrainian social media users to discredit her as a politician and hinder her political career.[64]

Related to gender disinformation is the phenomenon of terrorist radicalisation on the internet. There is a consensus in the literature on extremist violence that the internet is an "accelerator" of radicalisation, as extremist ideas become normalised within a community of individuals who validate each other; moreover, scholars in masculinities have recognised that individuals who perpetuate non-state political violence are overwhelmingly male, a common characteristic that extends across the ideological spectrum, making them more likely to be targeted and recruited by politically violent groups.[65] In particular, some of these online communities have been responsible for perpetuating cyberbullying against women, with doxxing and threats of physical and sexual violence being some of the most common tactics used to target feminist activists.[66] In this context, gender analysis of these threats is necessary as it would allow an understanding of the different appeals that the various internet platforms offer to these groups and, therefore, address some of the risks they present to peace and security.[67]

63. Judson, E., Atay, A., Krasodomski-Jones, A., & Smith, J. (2020). *Engendering hate: The contours of state-aligned gendered disinformation online*. Demos. https://apo.org.au/sites/default/files/resource-files/2020-10/apo-nid309184.pdf
64. Di Meco, L. (2019). *#SHEPERSISTED: Women, Politics & Power in the New Media World*. https://www.iknowpolitics.org/sites/default/files/191105shepersisted_final.pdf
65. Shoker, S. (2021). Op. cit.; Sharland, L., et al. (2021). Op. cit.
66. Shoker, S. (2021). Op. cit.
67. Sharland, L., et al. (2021). Op. cit.

C) DIFFERENTIAL VULNERABILITIES TO CYBER ATTACKS

Influenced by feminist, queer and racial studies perspectives on vulnerability, and thus in contrast to dominant technical security discourses that frame security as an objective or universal value and the "insecure user" as an objective state, Pierce et al.'s notion of "differential vulnerabilities" recognises that different populations and individuals have different types and degrees of digital security vulnerabilities and may be subject to miscellaneous attacks.[68] This concept, in turn, sidesteps the term "vulnerable populations", which can stigmatise and disempower individuals so labelled and construct a power relationship in which researchers, engineers or policy makers assume the role of protectors, which can contribute to reaffirming inequitable power relations. In this logic, differential vulnerability leads to a second related notion – that of differential trust – in that who trusts whom and for what purpose depends mainly on which users need to be protected and their position within particular groups and social contexts. In this context, differential vulnerabilities attributed to gender have enjoyed considerable prominence, as will be seen even in the field of traditional cybersecurity.

In general, there are two dominant ways so far of considering the various differential vulnerabilities based on gender.

Internet access and digital skills

The most recent global data from the International Telecommunication Union (ITU)[69] shows that an average of 62% of men use the internet worldwide, compared to 57% of women. Although the digital gender gap has been narrowing in all regions of the world and has been virtually eliminated in the developed world (89% of men and 88% of women are connected), significant gaps remain in less developed countries (31% of men vs. 19% of women) and in landlocked developing countries (38% of men vs. 27% of women). In addition, the gender gap remains particularly pronounced in Africa (35% of men versus 24% of women) and the Arab states (68% of men versus 56% of women).

68. Pierce, J., Fox, S., Merrill, N., & 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*. https://doi.org/10.1145/3274408
69. International Telecommunication Union. (2021). *Measuring digital development: Facts and figures 2021*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

However, the continuing decline in broadband connection prices and device costs has not prevented people, once connected, from lacking the necessary skills to take advantage of this technology to improve their lives. Moreover, according to EQUALS and UNESCO, there is ample evidence of the severity of the current gender gaps in digital skills: globally, women are less likely to know how to operate a smartphone, navigate the internet, use social networks and understand how to safeguard information in digital media.[70] Further, ethnographic studies conducted in countries and communities point to the fact that patriarchal cultures often prevent women and girls from developing digital skills. More worryingly, gender gaps in digital skills appear to be increasing as technologies become more sophisticated and expensive, despite interventions over at least two decades to move closer to gender equality.

The gendered lack of digital skills puts women at particular vulnerability when it comes to managing their cybersecurity. As seen in the UNESCO and EQUALS special report on the gender gap in digital skills,[71] in many contexts, women and girls face concerns of physical violence if they own or borrow digital devices, which in some cases leads them to use them in secret, making them more vulnerable to online threats and compounding the difficulty of acquiring digital skills. In addition, offline women are particularly at risk if exposed to empty threats and impersonation schemes common in the digital world. Women who lack digital skills may also be unaware that aggressors could use technology to control them. In this sense:

> Women need digital competence to ensure their safety, both online and offline. Knowledge of how to protect personal data and ensure privacy online is important for all internet users but is particularly salient for women and girls, who are more likely to be the targets of internet crimes and gender-based online violence.[72]

Other feminist researchers believe that the access and digital skills gap for women has to do with power dynamics and structural imbalances, as access is provided through the state and its apparatus, and then controlled through other sites of power, whether by large corporations and institutions such as the school or university, or the family,[73] spaces that often perpetuate hegemonic views of technologies.[74]

Demographic factors in cybersecurity behaviour

The inclusion of human interactions in cybersecurity has led many researchers in the field of "behavioural information security" to focus on studying the human layer and its vulnerability to cyber attacks, which can be produced by negligence,

70. West, M., Kraut, R., & Chew, H. E. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. EQUALS & UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000367416
71. Ibid.
72. Ibid.
73. van der Spuy, A., & Aavriti, N. (2018). *Mapping research in gender and digital technology*. APC. https://www.apc.org/en/pubs/mapping-research-gender-and-digital-technology
74. Zanolli, B., Jancz, C., Gonzalez, C., Araujo dos Santos, D., & Prado, D. (2018). Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018: Community Networks*. IDRC & APC. https://giswatch.org/sites/default/files/gw2018_t7_feminist_infrastrucutre.pdf

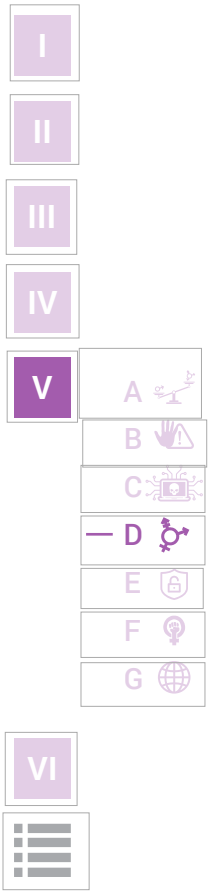
mistakes, illness, death, insider threats, and susceptibility to social engineering.[75] In other words, security countermeasures must take into account socio-technical aspects, beyond technical controls,[76] as understanding individual differences in cybersecurity behaviours helps researchers, organisations and employees working in the security sector to comprehend the sensitivity to potential security attacks.[77]

In this context, the analysis of demographic aspects of individuals, such as age, gender or educational background, seeks to provide clues about security behaviours, even if they are not always analysed from the context of power relations and social hierarchies as in intersectional theory. In this context, much of this research has revealed evidence of gender differences around cybersecurity beliefs and behavioural intentions, in addition to drawing on psychological factors to explain behaviours related to the cybersecurity domain.[78] Thus, the results are varied: for some, women's self-efficacy concerning cybersecurity is lower than men's; others show that women's level of awareness of personal data protection is lower than men's; some point to women's software updating behaviour being higher than men's, and some even point to a relationship between women's emotional instability and being more vulnerable to phishing.[79] In this context, the role of gender in cybersecurity behaviours is still unclear and needs to be further examined.[80] Nevertheless, these results, in addition to their methodologies, should be examined with care, especially when they do not make room for the contributions of intersectional gender theory that could help to complexify the look and avoid falling into the biologisation and universalisation of cultural differences between males and females. Some critical voices point out, for example, that:

> The literature surrounding sex and security behaviour has been mixed, with some researchers finding sex differences whilst others found none. We argue that any difference hypothetically present would be a socially constructed one, not a genetically caused one, and, as such, it necessitates looking toward sex-typed characteristics as the expression of idealised gender expression rather than looking at sex alone.[81]

75. Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human Risk Factors in Cybersecurity. *SIGITE '19: Proceedings of the 20th Annual SIG Conference on Information Technology Education*. https://doi.org/10.1145/3349266.3351407
76. Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures, computers & security. *Computers & Security, 97*. https://doi.org/10.1016/j.cose.2020.101931
77. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015
78. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040
79. Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies, 10*(4). https://doi.org/10.36941/ajis-2021-0111
80. McGill, T. J., & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. In *Australasian Conference on Information Systems 2018*. University of Technology Sydney ePress. https://dx.doi.org/10.5130/acis2018.co
81. Hull, M. (2015). *Factors affecting secure computer behaviour*. Master's thesis, Carleton University. https://curve.carleton.ca/system/files/etd/d2e61738-e6e1-4f3d-8e6e-aa1ba1bc7d38/etd_pdf/3c351dac4dd33a4bf5057bdcc66e1366/hull-factorsaffectingsecure-computerbehaviour.pdf

D) DIFFERENTIAL IMPACT OF CYBER INCIDENTS BASED ON GENDER

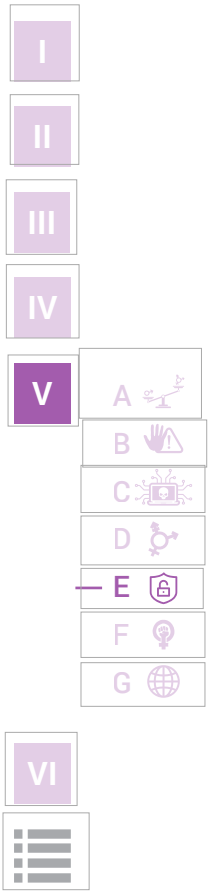


People experience online threats differently based on their identities and experiences, so it is necessary to understand that what is considered a "threat" in cybersecurity has gendered considerations. In other words, "traditional" threats in cybersecurity, such as espionage, economic theft, intrusion or disruption of personal devices and networks, have differentiated consequences based on the gender of the individuals affected, among other intersectional factors.[82] Likewise, it is recognised that attacks that constitute gender-based violence on the internet, such as doxxing, cyberbullying, and non-consensual dissemination of intimate images, are also threats that can arise from the intrusion or disruption of personal devices and networks.[83]

A classic case in the analysis is the differentiated affectations of personal data leakage. That is, with the understanding that data collection never takes place in a gender-neutral environment, when data breaches occur, they may have a more severe impact on women and LGBTIQ people due to historical and structural inequalities in power relations based on gender and sexuality.[84] Another phenomenon that has been widely analysed is the state's attempts to manage and govern networks, in which increasingly common internet outages create particular vulnerabilities for women and marginalised communities. Thus, it has been documented how internet shutdowns have a particularly adverse effect on women who, in their local realities, cannot have a presence in traditional public spaces, so not having access to the internet and their consequent lack of access to information is directly detrimental to their rights and freedoms.[85] In Uganda, for example, the internet shutdowns affected their essential role in national development as it is urban women who regularly access development programmes online.[86] Indeed, Brown and Pytlak identify the consequences of internet shutdowns on the personal safety of women and LGBTIQ people who use their mobile devices and communication channels as a security tool, the economic and professional costs paid by women in formal and informal economies, the effects on emotional well-being and, of course, at the educational level when women are relegated from traditional spaces, and the internet becomes an opportunity to access education.[87]

82. Brown, D., & Pytlak, A. (2020). Op. cit.; Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
83. Millar, K., Shires, J., & Tropina, T. Op. cit.
84. Brown, D., & Pytlak, A. (2020). Op. cit.
85. Johri, N. (2020, 13 November). India's internet shutdowns function like 'invisibility cloaks'. *DW*. https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554
86. Aceng, S. (2020, 15 December). Internet Shutdowns: An Evaluation of Women's Online Expression and Participation in Uganda. *The GNI Blog*. https://medium.com/global-network-initiative-collection/internet-shutdowns-an-evaluation-of-womens-online-expression-and-participation-in-uganda-8a4cac7bc479
87. Brown, D., & Pytlak, A. (2020). Op. cit.

E) RECONFIGURING CYBERSECURITY ANALYSIS FRAMEWORKS



Security analyses in cybersecurity typically begin with "threat modelling": a systematic analysis of the profile of the likely attacker, the most likely attack vectors, and the assets most desired by an attacker. Thus, for Slupska, threat modelling would reflect assumptions about the causes of insecurity among technology users.[88] But, as evidenced, people experience online threats differently depending on their identities and experiences. As such, many research papers are moving forward in creating new cybersecurity frameworks (using the basic pillars of design, defence and response prevalent among practitioners and policy makers), advancing in including gender considerations within those elements.[89] In this way, cybersecurity research that engages meaningfully with heretofore underserved groups could enable the development of cybersecurity systems designed to be more resilient to the range of threats that humans actually experience.[90]

On the one hand, there is the design pillar which, as stated by Millar et al., seeks to incorporate security into socio-technological systems to prevent or mitigate vulnerabilities and attacks.[91] The conception of cybersecurity employed in technological design is gendered, given that threat models, user notification and control procedures, and the advertising of cybersecurity technologies, mean that women (or gender groups in a more vulnerable position in a particular context) are more likely to have cybersecurity threats minimised or omitted;[92] to have more additional security burdens; and to more likely be affected by cybersecurity advertising that is disingenuous in the dangers to them.[93] Mindful of this reality as technical mitigation strategies will not comprehensively "solve" technology abuse problems in the context of gender-based violence perpetrated through the IoT, Slupksa and Tanczer believe that rather than seeking to eliminate all sources of vulnerability, it is more advantageous for industry players to think in terms of beneficial design patterns that, for example, advance design usability for those who are abused and make it more difficult for those who perpetrate abuse.[94] Also, the technology sector should be flexible enough to modify and redesign systems after implementation, which would benefit victims/survivors of gender-based violence and mainstream users because of

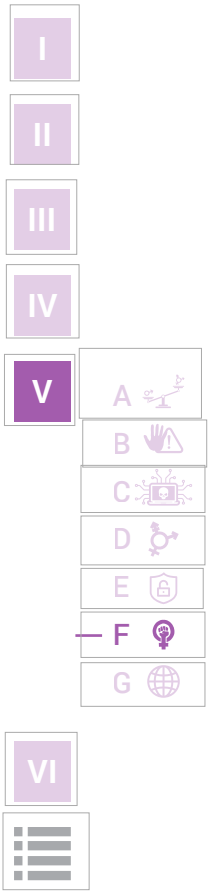
88. Slupska, J. (2019). Op. cit.
89. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
90. Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.
91. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
92. Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.
93. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
94. Slupksa, J., & Tanczer, L. (2021). Op. cit.

the security and privacy improvements that can be designed and implemented. There is also consensus on the need for the design pillar to be participatory, i.e. deploying methodologies to listen to citizens' concerns to broaden the scope of cybersecurity threat modelling. For Slupska, Dawson Duckworth, Neff et al., it is about creating threat modelling for humans rather than systems.[95]

Millar et al. further advance how gender influences the defence and incident response pillars.[96] In the former, due to its military roots, there are norms highly associated with masculinity, so prioritisation of the idea of cybersecurity for states and corporations occurs, leaving people behind. Gender norms around vulnerability can make it difficult to admit mistakes, seek help or work cooperatively, creating a reluctance to effectively implement cybersecurity defences and improve transparency around cybersecurity incident disclosure. At the incident response stage, there are several aspects from a gender perspective that should be considered: the priority given to attacks that are corporate over those affecting individuals, the way help is provided through highly coded language, the re-victimisation of victims (e.g. by blaming them for attacks), or the very over-masculinised composition of Computer Emergency Response Teams (CERTs or CSIRTs).

95. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). Op. cit.
96. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.

F) FEMINIST AUTONOMOUS INTERNET INFRASTRUCTURE

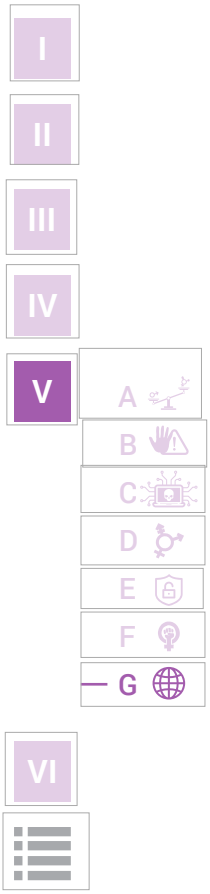


The contemporary internet infrastructure is designed and thought out in a way that barely takes into account situated experiences, which also explains why commercial platforms perpetuate long-established forms of violence against women, offering limited tools to address them adequately; in other words, most of the techno-political choices and relationships behind these devices do not address the needs of groups affected by structural inequalities, such as those of gender, race, ethnicity and class.[97] In response to this reality, feminism turns to the internet infrastructure in order to break with universalisations and relieve the local and situated experiences with partnerships and the exchange of knowledge and techniques.[98] The design and development of autonomous infrastructures seek to build independence and alternative economic systems, exchange, growth, work, and mutual care and respect.[99] Moreover, Prado et al. point out that adding the word "feminist" to infrastructures and proposing the intersectional perspective or social solidarities highlights the non-neutrality of technologies and devices that serve the functioning of the internet.[100] It also proposes a shift in the approach to cybersecurity: from one centred on the importance of individual privacy and the need to protect and defend against attacks to a collective framework of care and ethics within and outside communities. Notably, it indicates the need to build spaces – online and offline – free from attacks, where the freedom of expression of women, Black populations and LGBTIQ people, among others, must be guaranteed.[101]

A crucial part of this feminist infrastructure is the development of community networks. Along the lines of autonomous feminist infrastructure, these community networks challenge androcentrism and colonialism and criticise the hegemonic idea that these networks are only conceived for access without taking into account protocols, software and infrastructure design, in addition to other collective actions that seek the welfare of women in their diversity.[102]

97. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Tecnologias, infraestruturas e redes feministas: potências no processo de ruptura com o legado colonial e androcêntrico. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590003; Lobato, L. C., & 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
98. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Op. cit.
99. van der Spuy, A., & Aavriti, N. (2018). Op. cit.
100. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Op. cit.
101. van der Spuy, A., & Aavriti, N. (2018). Op. cit.; Zanolli, B., Jancz, C., Gonzalez, C., dos Santos, D. A., & Prado, D. (2018). Op. cit.
102. Zanolli, B., Jancz, C., Gonzalez, C., dos Santos, D. A., & Prado, D. (2018). Op. cit.

G) INTERNATIONAL PUBLIC POLICIES ON CYBERSECURITY



It is noteworthy to highlight the impetus that agendas such as the Women, Peace and Security (WPS) Agenda have given to gender in international public policy on cybersecurity.

For some time now, feminist researchers in international relations have questioned conventional security studies for their binary approaches to i nternal/external and personal/political violence and their view of conflicts from a top-down or structural perspective. In contrast, feminists have generally taken a bottom-up approach to analyse the impact of war at the micro-level.[103] Along these lines, the WPS Agenda has built a consensus on how women are uniquely and disproportionately affected by conflicts and other threats to international peace and security.[104]

Despite all these advances, human rights and "international security" are sometimes kept separate, meaning that while human rights should be a consideration when discussing international cybersecurity, the reality is that this has rarely been the case. As a result, less is known about how malicious international cyber operations between states affect people differently based on gender or other characteristics that may put them at risk of vulnerability.[105] Moreover, despite evidence that inequality and discrimination underlying people's gender and other intersectional intersections also influence the level of consequences experienced when facing a cyber incident, the WPS framework has not been systematically applied to cyberspace, so there is little data on how this differential impact in the ICT domain can be better understood and addressed in the context of international security.[106]

However, little by little, multilateral processes on cybersecurity have recently started to include official statements drawing attention to gender dimensions, but still in an overly timid and limited manner, as was the case in the final report of the UN Open-ended Working Group on cybersecurity. Indeed, despite the fact that several delegations had stated the need to mainstream gender in the implementation of cyber standards, build gender-sensitive capacities, and better understand the links between cybersecurity and gender equality frameworks, progress was unsatisfactory.[107]

103. Tickner, J. A. (2004). Op. cit.
104. United Nations. (2002). *Women, Peace and Security*. Study submitted by the Secretary-General pursuant to Security Council resolution 1325 (2000). https://www.un.org/womenwatch/daw/public/eWPS.pdf
105. Slupska, J. (2019). Op. cit.; Brown, D., & Pytlak, A. (2020). Op. cit.
106. Brown D., & Pytlak, A. (2020). Op. cit.; Sharland, L., et al. (2021). Op. cit.
107. Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor, 1*(10). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf

VI. CONCLUSIONS

This literature review has gathered information from diverse sources that work from different perspectives on gender in cybersecurity. These various approaches analyse gender from the context of unequal power relations as well as only a demographic factor. However, despite this vast diversity, it is possible to appreciate cross-cutting concepts of coincidence and particular themes where more evidence and studies are gathered. We have evidenced how more and more interest can be found in this topic, although a more or less ordered body of theory and practice is not yet apparent. In this context, this document proposes an ordering that can help organisations, academia and policy makers suggest their own maps of progress to deepen knowledge and/or increase the scope of knowledge in other areas of cybersecurity yet to be covered by a gender perspective.

BIBLIOGRAPHY

The following sources were consulted for this literature review:

Aceng, S. (2020, 15 December). Internet Shutdowns: An Evaluation of Women's Online Expression and Participation in Uganda. *The GNI Blog*. https://medium.com/global-network-initiative-collection/internet-shutdowns-an-evaluation-of-womens-online-expression-and-participation-in-uganda-8a4cac7bc479

Álvarez, D., & Vera, F. (2017). Ciberseguridad y derechos humanos en América Latina. In A. del Campo (Ed.), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Universidad de Palermo. https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Bardzell, S. (2010). Feminist HCI: Taking stock and outlining an agenda for design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. https://doi.org/10.1145/1753326.1753521

Barrett, F. J. (1996). The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy. *Gender, Work & Organisation, 3*(3), 129-142. https://doi.org/10.1111/j.1468-0432.1996.tb00054.x

Barsh, J., & Yee, L. (2011). *Unlocking the full potential of women in the US economy*. McKinsey & Company.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer, 52*(3), 58-6. https://doi.org/10.1109/MC.2018.2884190

Burrell, D. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1). http://dx.doi.org/10.4018/IJHIoT.2018010103

Brown, D., & Esterhuysen, A. (2019, 28 November). Why cybersecurity is a human rights issue, and it is time to start treating it like one. *APC*. https://www.apc.org/en/node/35879

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

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures, computers & security. *Computers & Security, 97*. https://doi.org/10.1016/j.cose.2020.101931

Collins, P. (2019). *Intersectionality as Critical Social Theory*. Duke University Press.

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human Risk Factors in Cybersecurity. SIGITE '19: *Proceedings of the 20th Annual SIG Conference on Information Technology Education*. https://doi.org/10.1145/3349266.3351407

Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32*(4), 411-424. https://doi.org/10.1017/S0892679418000618

Deibert, R. (2018). Trajectories for future cybersecurity research. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security*.

D'Hondt, K. (2016). *Women and Cybersecurity*. Master's thesis, Harvard Kennedy School.

Di Meco, L. (2019). *#SHEPERSISTED: Women, Politics & Power in the New Media World*. https://www.iknowpolitics.org/sites/default/files/191105shepersisted_final.pdf

Di Meco, L. (2020). *Online Threats to Women's Political Participation and The Need for a Multi-Stakeholder, Cohe-*

sive Approach to Address Them. UN Women. EGM/CSW/2021/EP8. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, 6(2), 22-30. https://www.cogitatiopress.com/politicsandgovernance/article/download/1385/1385

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies, 10*(4). https://doi.org/10.36941/ajis-2021-0111

EU Disinfo Lab. (2021, 24 May). Why Disinformation is a Cybersecurity Threat. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat

Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor, 1*(10). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Haciyakupoglu, G., & Wong, Y. (2021). *Gender, Security and Digital Space: Issues, Policies, and the Way Forward*. S. Rajaratnam School of International Studies. https://www.rsis.edu.sg/rsis-publication/cens/gender-security-and-digital-space-issues-policies-and-the-way-forward

Harris, B. A., & Woodlock, D. (2019). Digital Coercive Control: Insights from two landmark domestic violence studies. *The British Journal of Criminology, 59*(3), 530-550. https://doi.org/10.1093/bjc/azy052

Hull, M. (2015). *Factors affecting secure computer behaviour*. Master's thesis, Carleton University. https://curve.carleton.ca/system/files/etd/d2e61738-e6e1-4f3d-8e6e-aa1ba1bc7d38/etd_pdf/3c351dac4dd33a4bf5057bdcc66e1366/hull-factorsaffectingsecurecomputerbehaviour.pdf

International Telecommunication Union. (2021). *Measuring digital development: Facts and figures 2021*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

(ISC)². (2021). *In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity*. https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx

Johri, N. (2020, 13 November). India's internet shutdowns function like 'invisibility cloaks'. *DW*. https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554

Judson, E., Atay, A., Krasodomski-Jones, A., & Smith, J. (2020). *Engendering hate: The contours of state-aligned gendered disinformation online*. Demos. https://apo.org.au/sites/default/files/resource-files/2020-10/apo-nid309184.pdf

Kazansky, B. (2021). 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720985557

King-Close, A. M. (2016). *A gender analysis of cyber war*. Master's thesis, Harvard Extension School.

Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: The role of civil society. *Journal of Cyber Policy, 6*(3), 375-393. https://doi.org/10.1080/23738871.2021.1909090

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*. https://doi.org/10.1145/3322276.3322366

Lobato, L. C., & 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

McGill, T. J., & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. *In Australasian Conference on Information Systems 2018*. University of Technology Sydney ePress. https://dx.doi.org/10.5130/acis2018.co

Millar, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: Design, defence and response*. United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

Myrttinen, H. (2020). *Tool 1: Security Sector Governance, Security Sector Reform and Gender*. DCAF, OSCE/ODIHR & UN Women. https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

Nieminen, L. (2021). *Why is human trafficking excluded from the EU's cybersecurity?: An explorative study about cybersecurity and human trafficking in the European Union*. http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9698

Nissenbaum, H. (2005). Where computer security meets national security. E*thics and Information Technology, 7*, 61-73. https://doi.org/10.1007/s10676-005-4582-3

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (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)*. https://doi.org/10.1145/3368860.3368861

Pierce, J., Fox, S., Merrill, N., & 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*. https://doi.org/10.1145/3274408

Poster, W. R. (2018, 26 March). Cybersecurity needs women. *Nature*. https://www.nature.com/articles/d41586-018-03327-w

Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Tecnologias, infraestruturas e redes feministas: potências no processo de ruptura com o legado colonial e androcêntrico. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590003

Pytlak, A. (2021). Bringing gender analysis into international cybersecurity. *Cyber Peace & Security Monitor, 1*(8). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.8.pdf

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Information Security for South Africa 2014*. https://ieeexplore.ieee.org/document/6950492

Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03

Shoker, S. (2021). *Making gender visible in digital ICTs and international security*. Report submitted to Global Affairs Canada. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/research-canada-1.pdf

Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*. A/HRC/38/47. https://undocs.org/A/HRC/38/47

Šimonović, D. (2018). *Report of the Special Rapporteur on violence against women, its causes and consequences on violence against women in politics*. A/73/301. https://undocs.org/A/73/301

Slupska, J. (2019). Safe at Home: Towards a feminist critique of cybersecurity. *St. Anthony's International Review, 15*. https://ssrn.com/abstract=3429851

Slupska, J., Dawson Duckworth. S., Ma, L., & Neff, G. (2021). Participatory threat modelling: Exploring paths to reconfigure cybersecurity. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411763.3451731

Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). *Reconfigure: Feminist Action Research in Cybersecurity*. Reconfigure Network. https://www.oii.ox.ac.uk/news-events/news/reconfigure-feminist-action-research-in-cybersecurity

Slupska, J., & Tanczer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In J. Bailey, A. Flynn & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211049

Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review, 16*(1), 43-48. https://doi.org/10.1080/1040265042000210148

UNIDIR. (2021). *Fact sheet: Gender in cyber diplomacy*. https://unidir.org/publication/fact-sheet-gender-cyber-diplomacy

United Nations. (2002). *Women, Peace and Security*. Study submitted by the Secretary-General pursuant to Security Council resolution 1325 (2000). https://www.un.org/womenwatch/daw/public/eWPS.pdf

van der Spuy, A., & Aavriti, N. (2018). *Mapping research in gender and digital technology*. APC. https://www.apc.org/en/pubs/mapping-research-gender-and-digital-technology

Wajcman, J. (2000). Reflections on Gender and Technology Studies: In What State is the Art? *Social Studies of Science, 30*(3), 447-464. https://doi.org/10.1177/030631200030003005

West, M., Kraut, R., & Chew, H. E. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. EQUALS & UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000367416
Zanolli, B., Jancz, C., Gonzalez, C., Araujo dos Santos, D., & Prado, D. (2018). Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018: Community Networks*. IDRC & APC. https://giswatch.org/sites/default/files/gw2018_t7_feminist_infrastrucutre.pdf

Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS