CC-DRIVER

Researching cybercriminality to design new methods to
prevent, investigate and mitigate cybercriminal behaviour.

# Policy Brief No. 5

October 2022

## Who is this for?

The European Commission (REA, DG HOME), the CC-DRIVER Stakeholder Board, the CC-DRIVER Security Advisory Board, the CC-DRIVER Ethics Advisory Board

LEAs, policymakers, as well as private sector, non-profit and non-governmental organisations; especially those associated with cybercrime and cybersecurity

## Highlights

1. Cybersecurity failure is among the top ten global risks and one of those risks that has worsened most during the COVID-19 pandemic, meanwhile we are facing a growing skills shortage in the cybersecurity field.

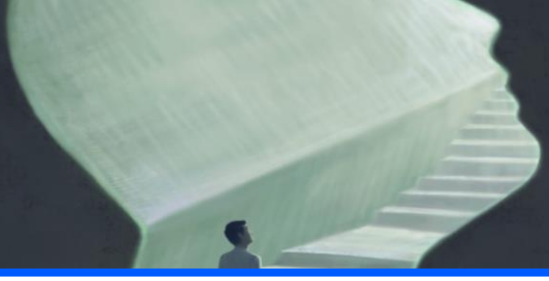
2. Women are affected twofold in cyber: They are more likely to be victims of cybercrime than men and women's representation in the cybersecurity workforce is disproportionately low.

3. Cyber harassment is seldomly covered by criminal law and prosecutions for online crimes are highly unlikely. Changes on a legal level are inevitable to criminalise malicious cyber behaviour.

4. Cybersecurity research and design needs to reflect the reality of women as prime targets of cybercrime, acknowledging that it's mostly (former) intimate partners who offend.

5. Women need to be empowered, motivated, educated and anchored to a cybersecurity career and the field of cybersecurity itself needs to implement changes to make it more appealing to women.

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



# Women in cyber

Cybersecurity failure is among the top ten global risks and one of those risks that has worsened most during the COVID-19 pandemic. Many countries and industries were able to adapt quickly to new forms of human interaction and remote work, but it came at the price of increased vulnerability to cyber threats.[1] This rather alarming state is exacerbated by a growing skills shortage in the cybersecurity field.[2]

Providing a cybersecure world is a crucial global challenge for the next years and to reach it, it is hugely important that we consider the bigger picture and disengage from the masculine stereotypes that have been dominant in the cybersecurity field for many years.[3] These stereotypes affect women in cyber twofold: as victims as well as professionals.

## Cybersecurity failing women

Women and girls are more likely to be victims of cybercrime than boys and men.[4,5,6] Digital discrimination can be inflicted by other humans, but it is also cybersecurity technology that may put women at a disadvantage: Biometric software, for example, has more trouble recognising female faces than male ones.[4]

Technological discrimination against women is grounded in the design of “smart” devices: they are conceptualised for male users. They do not take different needs of women into account, and neither varying kinds of uses that emerge from these needs—favouring what in society is perceived a masculine practice. These general issues of technological bias also specifically apply to cybersecurity.[7]

Additionally, women are expected to be perfect users, exercising near-total control over their digital footprint. This expectation, of course, are impossible to meet—for anyone. But when women fall victim to cybercrime, society blames them rather than acknowledging that in reality expectations towards use of cybersecurity measures are gendered.[7]

## Female professionals in cybersecurity

Gender equality is one of the 17 Sustainable Development Goals of the United Nations.[8] Women’s representation in the cyber workforce, however, is disproportionately low.[9] Equalising this gender imbalance would mean a step towards the UN’s goal of “peace and prosperity for people and the planet”[8] and also counter the projected skills shortage.

But why is there a gender gap in the cybersecurity profession?

1) Few women enter the field.
    - Barriers begin with the marketing of cybersecurity jobs, which is not gender-inclusive but overrepresents men. Women hence do not picture themselves doing the job, and therefore don’t apply.
    - Women tend to feel less confident regarding their skills. (While they are actually likely to be better qualified; regarding their level of expertise as well as their width of expertise.[4]) And, unlike men, they are less likely to apply for positions for which they do not feel completely qualified[10].

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

   - The cybersecurity profession is heavily stereotyped. Stereotypes represent young, white, loner-type males working all night.[10,11] Managers are more likely to hire persons fulfilling these stereotypes instead of (married) women (with children, of any colour, and of all ages), even when the woman's qualifications are superior.
   - And the mere fact itself of men being overrepresented in cybersecurity poses a hindrance for women to enter.[10]

2) Women are more likely to leave a job in cyber than men.
   - Women who did cope with stereotypes and discrimination during the hiring process, still have to overcome them on an everyday basis for a career in cybersecurity.[4,9,10]
   - A work environment expecting staff to be available 24/7 is particularly hard for women when they oftentimes are also expected to simultaneously take care of household and (little) children, especially in the early years of a woman's career.
   - Women—in a men's world—face more difficulties in finding a mentor and building a network of peers, which are essential to establish trust within a company, to being able to challenge superiors in cases where perspectives diverge, and generally to successfully navigate corporate settings.[9]

# Recommendations

### Law

Cyber harassment is seldomly covered by criminal law and prosecutions of online crimes are highly unlikely. Changes are necessary to criminalise malicious cyber behaviour.[12,13] Inclusion of online offences, such as cyberflashing, in criminal law can combine tort remedies, criminal prosecutions, and civil rights claims[12] or be based upon one of these models:

- consent-based model—criminalising all non-consensual online behaviour
- motivation-based model—criminalising all online behaviour with malign motives
- a combination of (1) and (2)[13]

### Technology

Cybersecurity research and design needs to reflect the reality of women as prime targets of cybercrime, acknowledging that it's mostly (former) intimate partners who offend. The most common tech abuse threats to consider are:[14]

- ownership-based access—being owner allows a perpetrator to prohibit usage or track locations/actions
- account/device compromise—guessing or coercing credentials to install spyware, monitor, steal data or lock victim out of their account
- harmful messages—contacting directly or indirectly via friends/family/employer without consent
- exposure of information—posting or threatening to post private information or images
- gaslighting—using a device's functions to make a victim doubt her own sanity

### Education

Girls and women need to be empowered, motivated, educated and anchored to a cybersecurity career for which building a community of knowledge, inspiration, and mentorship is paramount. One example for such an effort is the CybHER program.[15]

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

### Work environment

The field of cybersecurity itself needs to realise changes:[4]

- Acknowledging women’s expertise. Historically, women have been sidelined in cybersecurity while nowadays, their expertise tends to be overlooked.
- Becoming a less dismissive work environment for women and determining new standards for hiring and promoting besides the typical “hacker persona”.
- Conveying a new self-conception. Less of “aggressive warriors defending” and more of “creating safe systems to protect humans” would not only describe the job better, but also make it more appealing to women.

***Author***
*Dr Agnes Hoechtl*
*University of Applied Sciences for Public Services in Bavaria – Department Police*

## References

[1] World Economic Forum, *The Global Risks Report 2022*, 17th Edition, 2022.

[2] Deloitte AG, 24 January 2022. https://www2.deloitte.com/ch/en/pages/risk/articles/women-in-cyber.html

[3] Khan, M. K., *Overcoming gender disparity in cybersecurity profession* [Policy brief], G20 Insights. https://www.g20-insights.org/policy_briefs/overcoming-gender-disparity-in-cybersecurity-profession/

[4] Poster, W. R., „Cybersecurity needs women”, *Nature*, Vol. 555, March 2018, pp. 577-581.

[5] European Institute of Gender Equality, *Cyber violence against women and girls*, 2017.

[6] Malwarebytes, *Demographics of cybercrime report*, 2021. https://www.malwarebytes.com/resources/2021-demographics-of-cybercrime-report/index.html

[7] Millar, K., J. Shires, and T. Tropina, *Gender approaches to cybersecurity: Design, defence and response*, United Nations Institute for Disarmament Research, Geneva, 2021.

[8] United Nations, Department of Economic and Social Affairs, „Sustainable development—the 17 goals“. https://sdgs.un.org/goals (31 January 2022).

[9] Bagchi-Sen, S., Rao, H. R., Upadhyaya, S., & Chai, S., “Women in cybersecurity: A study of career advancement”, *IT Professional*, September/October 2009, 46-53.

[10] James, S., *The underrepresentation of females in the United States cybersecurity workforce: A multiple-case study* [Doctoral dissertation], 2019.

[11] Corneliussen, H., *What brings women to cybersecurity? A qualitative study of women’s pathways to cybersecurity in Norway* [Conference article], EICC 2020: Proceedings of the European Interdisciplinary Cybersecurity Conference, Reims, France, 18 November 2020.

[12] Citron, D. K. „Law’s expressive value in combating cyber gender harassement“, *Michigan Law Review, 108*(3), March 2009, pp. 373-416.

[13] McGlynn, C., „Cyberflashing: Consent, reform, and the criminal law“, *The Journal of Criminal Law*, 2022, pp. 1-17.

[14] Slupska, J. & Tanczer, L. M., „Threat modelling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things” in J. Bailey, A. Flynn, & N. Henry, The Emerald International Handbook of Technology-Facilitated Violence and Abuse, Emerald Publishing Ltd., pp. 663-688.

[15] Rowland, P., Podhradsky, A., & Plucker, S., “CybHER: A method for empowering, motivating, educating and anchoring girls to a cybersecurity career path”, Proceedings of the 51st Hawaii International Conference on System Sciences, 2018, pp. 3727-3735.

## Further Reading

- https://www.ccdriver-h2020.com/post/women-in-cyber-part-i-cybersecurity-failing-women
- https://www.ccdriver-h2020.com/post/women-in-cyber-part-ii-female-professionals-in-cybersecurity
- https://www.ccdriver-h2020.com/post/women-in-cyber-part-iii-empowering-women-in-cyber

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.