Photo Credit: Getty Images

Cracking the Code:
Shattering the Cybersecurity Glass Ceiling

Written by: **Ginevra Fontana,** Edited by: **Maryam Sindi**

EU Regulation defines cybersecurity as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats". The relevance and popularity of this field has grown in recent years thanks to the increased digitalisation of business, and has eventually risen to prominence with the pivot to remote working during the COVID-19 pandemic. As with most STEM careers, cybersecurity-related positions are mainly male-dominated, yet there is margin for improvement and a need for women to join the field.

According to both the World Bank and the 2020 ENISA Report on Women in Cybersecurity, the underrepresentation of female professionals in the industry impacts the overall growth of businesses. In 2020, women represented only 7% of the cybersecurity workforce in the EU; at the global level, only 20% of cybersecurity professionals were women — despite the overall number of women in the workforce being closer to half. Additionally, the 2021 European Parliament resolution on closing the digital gender gap identified the need to have more women in leadership positions at the EU-wide level. Numerous publications and reports, both by private sector entities as well as public organisations, have been decrying the gender pay and skills gap since 2019, when it was indeed assessed that not only women, but also women of colour were disproportionately underrepresented in the cybersecurity realm. Though the number of women employed in cybersecurity has been increasing in

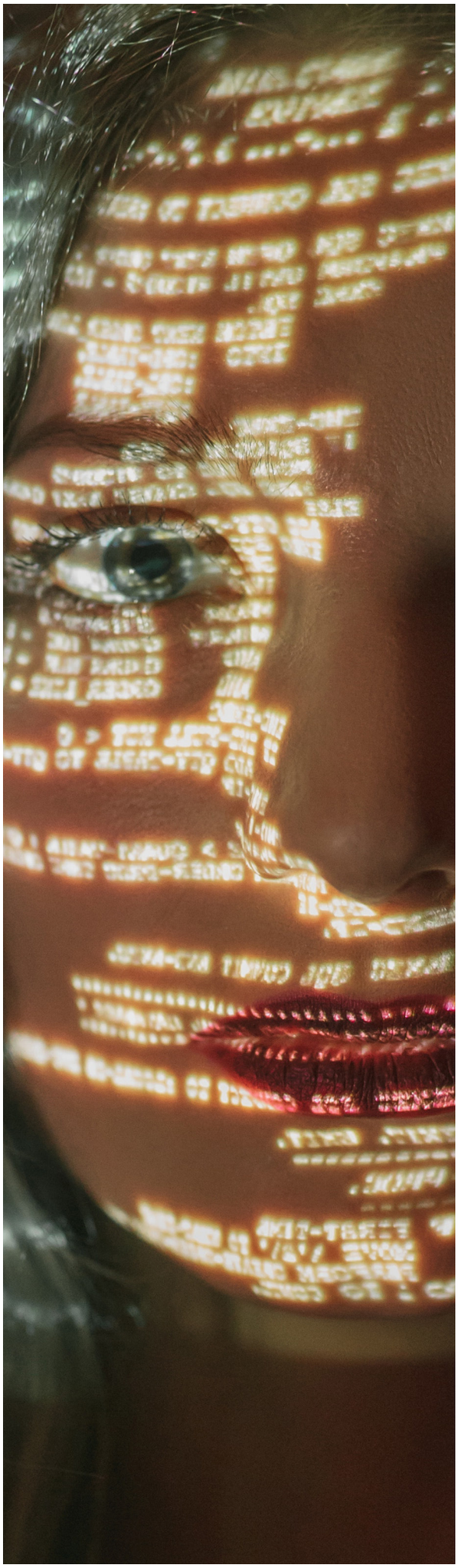

Photo Credit: Getty Images

recent years, with a promising double-digit increase between 2013 and 2019, the gap is far from being filled. The World Economic Forum recommended engaging even more girls and women in STEM, so as to keep up the increase in number and counter the predicted staff shortage. Non-governmental organisations and initiatives have also sprung up all over the world: from the US-based non-profit Women's Society of Cyberjutsu, to Karlie Kloss's Kode With Klossy, input has been given by women for women.

"In 2020, women represented only 7% of the cybersecurity workforce in the EU; at the global level, only 20% of cybersecurity professionals were women — despite the overall number of women in the workforce being closer to half."

Yet, it is undeniable that the inclusion of women in the cybersecurity workforce at large would benefit business, as they bring a new perspective to the table. It is also irrefutable that women have made history in cybersecurity: from their pioneering work in cryptography during World War II, to the female-led European Cybersecurity Forum (CYBERSEC), to Katie Moussouris's testimony on "Data Security and Bug Bounty Programs" at the US Senate in early 2018, women have been at the forefront of cybersecurity innovation and dialogue since its inception.

Women face the same issues within the cybersecurity realm that they already face elsewhere — lack of opportunities, the gender pay gap, workplace bias and discrimination, and difficulties in achieving a satisfactory work-life balance as they mostly act as primary caregivers for the children and elderly within their families. Women are also often overlooked for career advancement and promotions. The inadequate representation at all levels, but especially at the leadership ranks, makes it even more challenging for them to enter the field and advance their careers. It is also important to underline that, while these issues affect all women, they disproportionately impact more women of colour and non-binary people. Unfortunately, the lack of statistics and research on this topic hinders us from providing concrete numbers, and simply further highlights the need for more inclusivity in this field.

On top of all this, women and girls also have to contend with gender-based cyber-violence and hate speech. Women are more likely to be victims of non-consensual sharing of private images, blackmail, threats, stalking, defamation, as well as the establishment of fake profiles using their personal details, their pictures, or both. Another major issue that is often overlooked is the interconnectedness between online and offline crimes: online stalking is oftentimes linked to in-person behaviour. These risks feed into the negative perception of some women towards this field and, as such, might discourage them from pursuing careers in cybersecurity.

Naturally, one of the ways to solve all these issues and advance cybersecurity research and best practices would be by proactively pursuing a more diverse workforce and actively fighting against all forms of discrimination. The inclusion of multiple perspectives into a male-dominated industry would help to stimulate innovative and variegated solutions to any issues that will arise. Women should be encouraged and incentivized to pursue careers in cybersecurity, including both non-technical positions (e.g. governance and compliance) and technical roles which remain to be dominated by men.