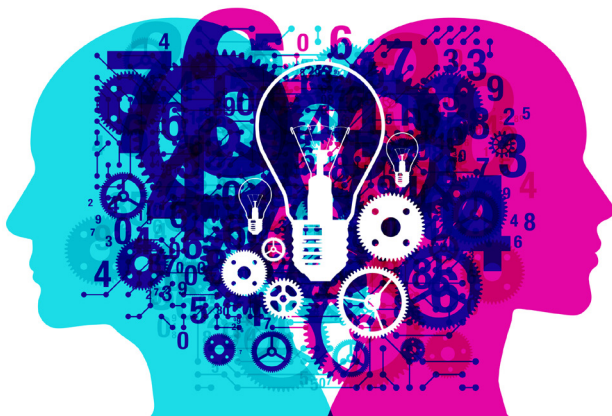


# WOMEN IN CYBER A MANIFESTO FOR TODAY



Currently, women represent only a minority of the workforce in the cybersecurity domain. The figures have increased over the years, but they are still far from reflecting a balanced representation of both genders. There are several reasons behind this lack of female presence. In addition to those in common with other STEM fields, we have to face the widespread perception of the cybersecurity as a male-dominated and highly specialised IT field, thus, not an appropriate field for women to enter into. This situation calls for actions to contribute towards a cultural shift in favour of a more inclusive approach that would be beneficial for the cybersecurity market and of the society as a whole.

On a broader perspective, the issue of diversity, also with respect to the particular domain of cybersecurity, pertains to the overarching issue of gender equality. Gender equality has been identified as one of the seventeen (17) Sustainable Development Goals (SDGs) included in the 2030 Agenda for Sustainable Development, which was adopted by world leaders in 2015. Gender equality has been ranked as the 5th SDG and it is considered to be integral to the entire set of the SDGs identified.



This Manifesto aims at achieving the following goals:

**1** Raise awareness about the cybersecurity culture, stressing its impact on society and state sovereignty and, therefore, its profound influence on one's everyday life. Same as other professions, young women should perceive cybersecurity as a career option assigned with a social role.

Increase awareness of the multidisciplinary nature of cybersecurity, which requires complementing skills and expertise, including the utilization of both hard skills and soft skills, and the cooperation between experts with different knowledge backgrounds such as IT, economics and social sciences.

**2**

**3** Promote positive role models, putting forward in a pragmatic manner how family life and a career in cybersecurity can be combined, thus, encouraging women towards a career in cybersecurity or allowing for a career reorientation.

To this end, this Manifesto adopts a holistic approach aiming at addressing the gender gap from different perspectives. In this respect, existing initiatives such as Women4Cyber, WomenENCourage and Concordia's Women in Cyber will implement concrete actions addressing the goals set out in this Manifesto across six (6) key areas and related actions, namely: education, entrepreneurship, industry, investment, legal/strategy and research.

# Education/Skills

Cybersecurity is a field that requires not only technical experts but proactive people with strong managerial and soft skills. This is where we can best engage with and attract girls and women to the profession and how we can ultimately fill the skills gap and ensure fair and equal representation in cybersecurity.

There is an urgent need to ensure that we are educating and training enough skilled experts to meet the demand. In addition to introducing cyber security as a multidisciplinary topic across education programmes, we need to attract more young people, girls in particular, to cybersecurity by demonstrating the multifaceted nature of the profession. We need to remove the misconception that cybersecurity is just a technical issue – it is about people and processes too.

# Entrepreneurship

According to the information encoded in the dealroom.co, out of almost 1600 startups and scaleups registered on the platform and acting in the cybersecurity field, one-third of them have their HQ registered in Europe, and a similar number is to be found in the US. Out of the 510 European cybersecurity companies, only 12 of them are led by women, four times less than in the US. Most of the 12 women-led cyber startups were setup in the last 15 years and are in the early growth stage.

We need to create a community of European women-led startups and innovations, by fostering the entrepreneurial spirit, best practices, and networking reach of women in cybersecurity today.

# Industry

One of the main challenges of the industry is the hiring of cyber resources (need to find the latest statistic). The demand for cyber specialists and experts is greater than the supply, and this is making society and organisations increasingly vulnerable. Cyber industrials are finding more and more difficult to recruit in sufficient numbers, but also in quality, the talents they need to develop out the cyber offers essential to their resilience of the private sector and the society, as well as the emergence of European industrial champions able to develop the European competitiveness. From a social standpoint, Industrials cannot bear that the cyber sector, whose impacts on our daily lives are increasing, to be thought, developed and governed only by men.

Thus there is a need for concrete actions to support a more inclusive, open and female-friendly environment in cybersecurity industries.

# Investment

PitchBook Data stated that since the beginning of 2016 companies with women founders had received only 4.4% of venture capital deals. Those companies have garnered only about 2% of all capital invested in the US. In Europe, the statistics are better but do not surpass 7%. There is a gender gap in the investments on women-led startups, in spite of the fact that all the data shows these startups, on average, have better ROI when invested and better performance in innovation and other variables. This figure is even more alarming if we consider that, according to Strategic Cyber Ventures, in 2018 we saw the record of \$5.3 billion in cybersecurity venture capital funding, an increase above 20% from 2017 (\$4.4 billion) and double that of 2016. These data call to actions to raise awareness on the great opportunity to invest in women-led cybersecurity startups. We need also to help create women-led business angels groups and networking infrastructure for investing in STEM and in Cybersecurity women-led startups facilitation capital access in early stages.

# Legal/Strategy

The European Charter of Fundamental Rights explicitly provides for the principle of equality between men and women in all areas including employment, work and pay; the Charter, also, provides for the " maintenance or adoption of measures providing for specific advantages in favour of the under-represented sex". In light of these regulatory obligations relevant for all Member States, employers are expected to take measures for equality to be ensured in reality, including, with respect to professions such as cybersecurity where the gender quotas are far from being balanced.

To this end, it is of critical importance that the European and the national policy makers take the necessary strategic decisions that will actually incentivise effective compliance with existing rules, thus, going beyond mere "box ticking".

# Research

According to data collected by the UNESCO Institute of Statistics (UIS), less than 30% of the world's researchers are women. Data shows a clear leaky pipeline, with a growing number of women pursuing bachelor's and master's degrees, but many opt-outs at PhD level, a required title for a research career. In computer science, this is even more alarming as data shows a regular decrease in female graduates since 2000, particularly evident in high-income countries. This trend accordingly appears in the cybersecurity field. This leaky pipeline impacts several research decision-making processes, with women being underrepresented as peer reviewers on editorial boards and research councils, and in having fewer leader positions in tertiary education and R&D.

This picture calls for activities to raise awareness on the importance of involving women in project and research teams, to recognise and prize the effort and good results of women, to work on the recognition of the profession researcher independent on the gender.