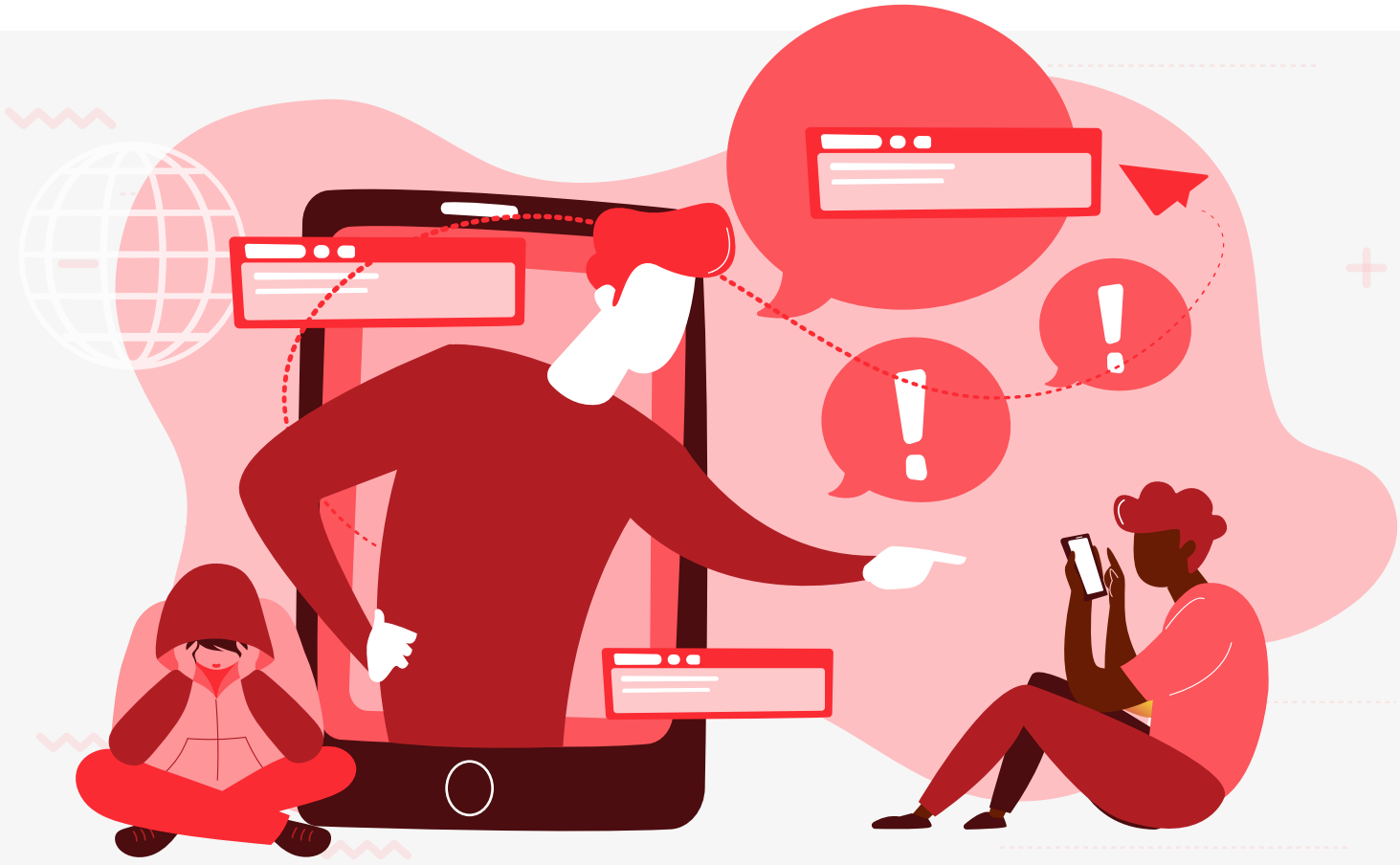
A Feminist Theorisation of Cybersecurity to Identify and Tackle Online Extremism

By Elsa Bengtsson Meuller

Global Network
on Extremism & Technology

The practice of online abuse is gendered and racialised in its design and works to assert dominance through male supremacist logic. Online abuse is often used by extremist groups such as the far right, jihadist groups and misogynist incels and disproportionately targets marginalised populations, particularly people of colour, women and transgender and non-binary people. Currently, online abuse is not seen as a 'threat of value' in cybersecurity policies or a priority within Preventing and Counter Violent Extremism (P/CVE) policies.



Through the implementation of a feminist theorisation of cybersecurity to tackle extremism, this report proposes three core shifts in our responses to online extremism:

1. Incorporate misogynist and racist online abuse into our conceptions of extremism.

2.Shift the focus from responding to attacks and violence to addressing structural violence online.

3. Empower and centre victims and survivors of online abuse and extremism.

Findings

A theorisation of feminist cybersecurity centred on victims of online abuse and extremism can help to tackle extremist violence and work to counter the structures of power from which extremism stems.

Policymakers need to refocus and evaluate whether they put disproportionately more resources towards identifying perpetrators than helping victims and survivors of violence.

The disengagement with gendered and racially oppressive structures within current P/CVE and cybersecurity areas means that strategies and activities that counter extremisms build on male supremacist logic and lack impactful intervention measures.